This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

09/674950
529 Rec'd PCT/PTC 07 NOV 2000

932.1173

UNITED STATES PATENT AND TRADEMARK OFFICE

Re: Application of: Angel José FERRE HERRERO

Serial No.: Not yet known

Filed: Herewith

For: RANDOMIZATION-ENCRYPTION SYSTEM

LETTER RE PRIORITY

Assistant Commissioner for Patents
Washington, DC 20231-9998

November 7, 2000

Dear Sir:

Applicant hereby claims the priority of Spanish Patent Application No. 9801037 filed May 7, 1998 and Spanish Certificate of Addition No. 9801398 filed June 22, 1998 through International Patent Application No. PCT/ES99/00115 filed April 30, 1999.

Respectfully submitted,

STEINBERG & RASKIN, P.C.

By: _____

Paul J. Higgins
Reg. No. 44,152

Steinberg & Raskin, P.C.
1140 Avenue of the Americas, 15th Floor
New York, NY 10036-5803
Phone: (212) 768-3800
Facsimile: (212) 382-2124
E-mail: sr@steinbergraskin.com

F:\H\932\1173\PROSECU\PRIO-LTR

THIS PAGE BLANK (USPTO)

09/674950
529 Rec'd PCT/PTC 07 NOV 2000

VERIFICATION OF A TRANSLATION

I, the below named translator, hereby declare that:

My name and post office address are as stated below:

That I am knowledgeable in the English language and in the language in which the below identified international application was filed, and that I believe the English translation of the International patent application No.PCT ES99/00115 is a true and complete translation of the above identified International application as filed.

I hereby declare that all statements made herein are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

30th SEPTEMBER, 2000

Dated

Montse R

Post Office Address

MONTSE REVERTER GARCIA
C/ AVD. CATALUNYA, 60
43540 ST. CARLES DE LA RAPITA
SPAIN

THIS PAGE BLANK (USPTO)

PCT ES 99/00115

9/674950

5ª.

REC'D 15 JUN 1999
WIPO PCT

OFICINA ESPAÑOLA

ES99/115

de

PATENTES y MARCAS

CERTIFICADO OFICIAL

Por la presente certifico que los documentos adjuntos son copia exacta de la solicitud de PATENTE ADICIONAL número 9801398 , presentada en este Organismo, con fecha 22 de Junio de 1998.

Madrid, 3 de junio de 1999

El Director del Departamento de Patentes
e Información Tecnológica.
P.D.

M. MADRUGA

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

THIS PAGE BLANK (USPTO)

P9801398

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

INSTANCIA DE SOLICITUD DE:

☑ PATENTE DE INVENCION ☐ MODELO DE UTILIDAD

NUMERO DE SOLICITUD

GENERALITAT DE CATALUNYA DEPARTAMENT D'INDUSTRIA, COMERÇ I TURISME

FECHA Y HORA DE PRESENTACION EN O.E.P.M.
22 JUNY 1998
CIDEM

FECHA Y HORA DE PRESENTACION EN LUGAR DISTINTO O.E.P.M.

(1)
☒ SOLICITUD DE ADICION
☐ SOLICITUD DIVISIONAL
☐ CAMBIO DE MODALIDAD
☐ TRANSFORMACION SOLICITUD EUROPEA

(2) EXPED. PRINCIPAL O DE ORIGEN
MODALIDAD PATENTE
NUMERO SOLICITUD 9801037
FECHA SOLICITUD 07/05/98
MODALIDAD
NUMERO SOLICITUD
FECHA SOLICITUD

(3) LUGAR DE PRESENTACION: BARCELONA — CODIGO 08

(4) SOLICITANTE(S) APELLIDOS O DENOMINACION JURIDICA	NOMBRE	DNI
FERRE HERRERO	ANGEL JOSE	40923966

OFICINA ESPAÑOLA DE PATENTES Y MARCAS
Dpto. SECRETARIA GENERAL
REPROGRAFIA
Panamá, 1 - Madrid 28071

(5) DATOS DEL PRIMER SOLICITANTE

DOMICILIO AVGDA. CONSTITUCIO, 3 BIS, 19
LOCALIDAD SANT CARLES DE LA RAPITA
PROVINCIA TARRAGONA
PAIS RESIDENCIA ESPAÑA
NACIONALIDAD ESPAÑOLA

TELEFONO 977740661
CODIGO POSTAL 43540
CODIGO PAIS ES
CODIGO NACION ES

(6) INVENTOR(ES) (7) ☒ EL SOLICITANTE ES EL INVENTOR ☐ EL SOLICITANTE NO ES EL INVENTOR O UNICO INVENTOR

(8) MODO DE OBTENCION DEL DERECHO ☐ INVENC. LABORAL ☐ CONTRATO ☐ SUCESION

APELLIDOS	NOMBRE	NACIONALIDAD	COD. NACION
FERRE HERRERO	ANGEL JOSE	ESPAÑOLA	ES

(9) TITULO DE LA INVENCION

MEJORAS EN LA PATENTE PRINCIPAL Nº9801037 POR: "DISPOSITIVO DE ALEATORIZACION-ENCRIPTACION DE SECUENCIA DE DATOS"

(10) INVENCION REFERENTE A PROCEDIMIENTO MICROBIOLOGICO SEGUN ART. 25.2 L.P. ☐ SI ☒ NO

(11) EXPOSICIONES OFICIALES
LUGAR ..... FECHA .....

(12) DECLARACIONES DE PRIORIDAD

PAIS DE ORIGEN	COD. PAIS	NUMERO	FECHA

(13) EL SOLICITANTE SE ACOGE A LA EXENCION DE PAGO DE TASAS PREVISTA EN EL ART. 162 L.P. ☐ SI ☒ NO

(14) REPRESENTANTE — APELLIDOS — NOMBRE — CODIGO
DOMICILIO — LOCALIDAD — PROVINCIA — COD. POSTAL

(15) RELACION DE DOCUMENTOS QUE SE ACOMPAÑAN

☒ DESCRIPCION. N.º DE PAGINAS... 31
☒ REIVINDICACIONES. N.º DE PAGINAS... 12
☒ DIBUJOS. N.º DE PAGINAS... 8
☒ RESUMEN
☐ DOCUMENTO DE PRIORIDAD
☐ TRADUCCION DEL DOCUMENTO DE PRIORIDAD
☐ DOCUMENTO DE REPRESENTACION
☐ PRUEBAS
☒ JUSTIFICANTE DEL PAGO DE TASAS
☐ HOJA DE INFORMACIONES COMPLEMENTARIAS
☐ OTROS

FIRMA DEL FUNCIONARIO

FIRMA DEL SOLICITANTE O REPRESENTANTE

(16) NOTIFICACION DE PAGO DE LA TASA DE CONCESION

Se le notifica que esta solicitud se considerará retirada si no procede al pago de la tasa de concesión; para el pago de esta tasa dispone de tres meses a contar desde la publicación del anuncio de la concesión en el BOPI, más los diez días que establece el art. 81 del R.D. 10-10-86.

ILMO. SR. DIRECTOR DE LA OFICINA ESPAÑOLA DE PATENTES Y MARCAS

1. O.E.P.M. Expediente

CUMPLIMENTAR LOS TRES EJEMPLARES SALVO ZONAS EN ROJO

THIS PAGE BLANK (USPTO)

PATENTE
RESUMEN Y GRAFICO

NUM DE SOLICITUD P9801398

FECHA DE PRESENTACION

RESUMEN (Máx. 150 palabras)

Mejoras en la patente principal nº 9801037 por: "Dispositivo de aleatorización-encriptación de secuencia de datos".

Se caracterizan porque el bloque (WTI) agrupado en unidad de agrupación (603) con bloque de datos (XI) dando como resultado interbloque (VI) es bloque transformador (WTI) generado en unidad de generación de bloque transformador (1002) haciendo uso de bloque inicial de control (R) y de bloque de salida (YI). Asimismo, dependiendo de la unidad de generación de bloque transformador (1002) particular que se implemente, el bloque de control (Kpv2) tiene longitud superior a la longitud del bloque de control del dispositivo de la patente principal.

En una segunda realización se ha previsto una unidad de generación de bloque transformador diferente con la que igualmente se hace uso de bloque de control (Kpv2) de mayor longitud.

GRAFICO

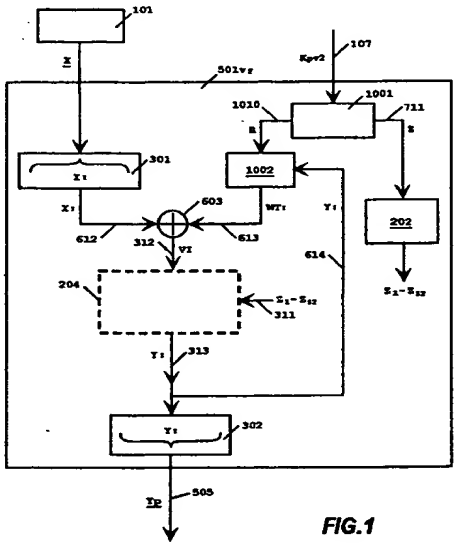

FIG.1

RESUMEN DE LA INVENCION Y GRAFICO

El resumen al que se refiere el artículo 27 de la Ley tendrá una extensión máxima de 150 palabras, deberá indicar el título de la invención y contener una exposición concisa del contenido de la descripción y reivindicaciones y, en su caso, dibujo o dibujos más característicos que deberán situarse debajo del texto del resumen.

El resumen deberá permitir una fácil comprensión del problema técnico planteado, la solución aportada y el uso o usos principales de la invención.

Los márgenes mínimos serán los siguientes:

Izquierdo: superior 2 cm.
Derecho: 2 cm.
Inferior: 2 cm.

Las dimensiones máximas del (de los) gráfico(s) serán 8 x 8 cm.

SPAÑOLA DE PATENTES
OFICINA Y MARCAS

(31) NUMERO (32) FECHA DATOS DE PRIORIDAD (33) PAIS

A1 (12) PATENTE DE INVENCION

(21) NUMERO DE SOLICITUD P 9801398

(22) FECHA DE PRESENTACION

(71) SOLICITANTE(S)
Don Angel José FERRE HERRERO

NACIONALIDAD
ESPAÑOLA

DOMICILIO
SANT CARLES DE LA RAPITA, TARRAGONA, Avgda Constitució, 3bis 3°

(72) INVENTOR(ES)
El solicitante

(73) TITULAR(ES)

(11) N.º DE PUBLICACION

(45) FECHA DE PUBLICACION

(62) PATENTE DE LA QUE ES DIVISIONARIA

(51) Int. Cl.

(54) TITULO

MEJORAS EN LA PATENTE PRINCIPAL Nº 9801037 POR: "DISPOSITIVO DE ALEATORIZACIÓN-ENCRIPTACIÓN DE SECUENCIA DE DATOS".

GRAFICO (SOLO PARA INTERPRETAR RESUMEN)

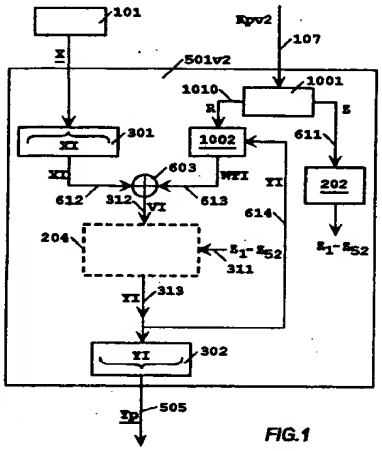

FIG.1

(57) RESUMEN (APORTACION VOLUNTARIA, SIN VALOR JURIDICO)

Mejoras en la patente principal nº 9801037 por: "Dispositivo de aleatorización-encriptación de secuencia de datos".

Se caracterizan porque el bloque (WTI) agrupado en unidad de agrupación (603) con bloque de datos (XI) dando como resultado interbloque (VI) es bloque transformador (WTI) generado en unidad de generación de bloque transformador (1002) haciendo uso de bloque inicial de control (R) y de bloque de salida (YI). Asimismo, dependiendo de la unidad de generación de bloque transformador (1002) particular que se implemente, el bloque de control (Kpv2) tiene longitud superior a la longitud del bloque de control del dispositivo de la patente principal.

En una segunda realización se ha previsto una unidad de generación de bloque transformador diferente con la que igualmente se hace uso de bloque de control (Kpv2) de mayor longitud.

DESCRIPCION

Mejoras en la patente principal nº 9801037 por: "Dispositivo de aleatorización-encriptación de secuencia de datos".

La memoria concierne a unas mejoras introducidas en el objeto de la patente principal nº 9801037 que se refiere a un dispositivo de aleatorización-encriptación de secuencia de datos tal que la secuencia resultado presenta substancialmente propiedades características de las secuencias de números aleatorios, con lo que la difusión y confusión presente en la secuencia aleatorizada-encriptada resultado es objetivamente medible permitiendo conocer la confusión y difusión que introduce la clave de aleatorización-encriptación usada. Las mejoras objeto del presente Certificado de Adición proceden de la investigación adicional llevada a cabo en el objeto de la Patente principal.

Las mejoras pretenden en primer lugar, aumentar la calidad del bloque de longitud N que se agrupa con el bloque de datos de longitud N para dar el interbloque de longitud N que se suministra como entrada de la unidad de encriptación-desencriptación. En el objeto de la patente principal el bloque de longitud N es el bloque de salida y, por lo tanto, tenemos que los ataques enemigos que intentan descubrir la secuencia de texto claro o la clave de aleatorización-encriptación usada, tienen conocimiento del bloque de longitud N en particular con el que es agrupado el bloque de datos de longitud N, elemento éste que puede ser de gran ayuda para lograr sus propósitos. Suministrando un bloque de longitud N generado por unos medios generadores de bloque transformador, tenemos que el bloque de datos de longitud N es agrupado con un bloque desconocido por los posibles adversarios, con lo que la vulnerabilidad de la confidencialidad de la información aleatorizada-encriptada se ve decrementada Asimismo, como consecuencia de la introducción de los medios generadores de bloque transformador, se puede conseguir que la longitud de la clave de aleatorización-encriptación se vea incrementada en función de la implementación específica de los mencionados medios generadores de bloque transformador, con lo que se incrementa la resistencia de la aleatorización-encriptación de la secuencia de texto ante ataques como los que se conocen por el nombre de "ataques por la fuerza bruta".

EXPLICACION

La presente memoria se centra en unas notables mejoras introducidas en el dispositivo de aleatorización-encriptación correspondiente a la patente principal nº 9801037.

El punto principal de las mejoras se centra en suministrar a los medios de agrupación, para ser agrupado con el bloque de datos de longitud N dando un interbloque de longitud N, el bloque transformador de longitud N, en substitución del bloque inicial de control de longitud N.

La obtención del bloque transformador de longitud N se consigue por:

- la introducción en el dispositivo de la patente principal de medios lógicos generadores de bloque transformador de longitud N, los cuales generan el bloque transformador de longitud N a partir de dos bloques, bloque de salida de longitud N y bloque inicial de control de longitud G;
- y la substitución de los medios divisores de bloque de control en bloque inicial de control de longitud 2N y bloque inicial de control de longitud N de la patente principal por medios divisores de bloque de control en bloque inicial de control de longitud 2N y, mencionado previamente, bloque inicial de control de longitud G. El mencionado bloque inicial de control de longitud G es suministrado desde los medios divisores de bloque de control a los mencionados medios lógicos generadores de bloque transformador de longitud N para la generación del bloque transformador de longitud N.

El suministro del bloque transformador de longitud N, generado por medios lógicos generadores de bloque transformador de longitud N haciendo uso del bloque inicial de control de longitud G y el bloque de salida de longitud N cuando éste es suministrado, a los medios de agrupación para ser agrupado con cada bloque de datos de longitud N permite conseguir las ventajas que se exponen a continuación. El bloque transformador de longitud N puede ser fácilmente no deducible en función de la implementación específica de los mencionados medios lógicos generadores de bloque transformador de longitud N y, a diferencia del dispositivo objeto de la patente principal nº 9801037, no es accesible como el bloque de salida de longitud N, el cual en la referida patente principal es utilizado como nuevo bloque inicial de control de longitud N para ser agrupado en los medios de agrupación; lo cual confiere una mayor

seguridad en la no vulnerabilidad de la información que se pretende proteger ante ataques enemigos. Asimismo, como segunda ventaja consecuencia de los cambios que se realizan para conseguir la mejora previamente descrita, el bloque inicial de control de longitud G, el cual se extrae del bloque de control y es suministrado a los mencionados medios lógicos generadores de bloque transformador de longitud N, tendrá longitud que dependerá de la implementación específica que se realice de los mencionados medios lógicos generadores de bloque transformador de longitud N, longitud que puede ser superior a la longitud del bloque inicial de control de longitud N del dispositivo de la patente principal nº 9801037, y por lo tanto, hacer uso el dispositivo con las mejoras incorporadas de un bloque de control de longitud superior a la longitud del bloque de control del dispositivo de la patente principal nº 9801037 con las ventajas que ello conlleva ante ataques enemigos como los que se conocen por "ataques por fuerza bruta".

Como es obvio, el dispositivo de desencriptación descrito en la patente principal nº 9801037, también incorpora las mejoras correspondientes que permiten llevar a cabo la desencriptación de los textos aleatorizados-encriptados haciendo uso del dispositivo con las mejoras incorporadas que han sido expuestas anteriormente.

Se ha previsto una segunda realización de las mejoras objeto de la presente memoria sobre el dispositivo de aleatorización-encriptación objeto de la patente principal nº 9801037, tal que incorporando el dispositivo esta segunda realización de las mejoras, el dispositivo continúa ofreciendo la funcionalidad propia del mismo, es decir, aleatorización-encriptación de secuencia de datos, lográndose además las ventajas previamente descritas al introducir la primera realización de las mejoras objeto de la presente invención.

En esta segunda realización de las mejoras el punto principal de las mismas se centra igualmente en el suministro del bloque transformador de longitud N, generado por medios lógicos generadores de bloque transformador de longitud N, a los medios de agrupación, para ser agrupado con cada bloque de datos de longitud N dando un interbloque de longitud N, en substitución del bloque inicial de control de longitud N. La diferencia con respecto a la primera realización de las mejoras estriba en que los medios lógicos generadores de bloque transformador de bloque de longitud N generan el bloque transformador de longitud N haciendo uso del bloque inicial de control de longitud G únicamente, no hacen uso del bloque de salida de longitud N. Obviamente,

respecto al dispositivo objeto de la patente principal, también en esta segunda realización al igual que en la primer realización de las mejoras, los medios divisores de bloque de control en bloque inicial de control de longitud 2N y bloque inicial de control de longitud N, son substituidos por medios divisores de bloque de control en bloque inicial de control de longitud 2N y bloque inicial de control de longitud G, bloque éste ultimo que es suministrado a los mencionados medios lógicos generadores de bloque transformador de longitud N.

Al igual que en la primer realización de las mejoras, el bloque transformador de longitud N no es fácilmente deducible ni es accesible, lo cual confiere una mayor seguridad en la no vulnerabilidad de la información que se pretende proteger ante ataques enemigos. Asimismo, también se consigue la ventaja referente a la posible mayor longitud del bloque inicial de control de longitud G que se suministra a los medios lógicos generadores de bloque transformador de longitud N, que aunque dependerá de la implementación específica que se realice de los mencionados medios lógicos generadores de bloque transformador de longitud N, puede ser también superior a la longitud del bloque inicial de control de longitud N del dispositivo de la patente principal nº 9801037, y por lo tanto, hacer uso el dispositivo de un bloque de control de longitud superior a la longitud del bloque de control del dispositivo de la patente principal nº 9801037 con las ventajas que ello conlleva ante ataques enemigos como los que se conocen por "ataques por fuerza bruta". En esta segunda realización de las mejoras, la principal diferencia con respecto a la primer realización de las mejoras radica en la eliminación de la realimentación, que se lleva a cabo en la mencionada primer realización, de los medios lógicos generadores de bloque transformador de longitud N con el bloque de salida de longitud N. Por ello, en esta segunda realización las posibilidades de que las secuencias aleatorizadas-encriptadas, resultado de la aplicación del dispositivo que incorpora esta segunda realización de las mejoras a una secuencia de datos, presenten substancialmente las características propias de las secuencias de números aleatorios, dependerá en gran medida de la implementación especifica que se realice de los medios lógicos generadores de bloque transformador de longitud N.

Para poder a cabo la desencriptación de los textos que han sido aleatorizados-encriptados haciendo uso del dispositivo de aleatorización-encriptación con esta segunda realización de las mejoras, es necesario también introducir las mejoras

correspondientes en el dispositivo de desencriptación.

A continuación para facilitar una mejor comprensión de esta memoria descriptiva y formando parte integrante de la misma se acompaña una serie de figuras en las que con carácter ilustrativo y no limitativo se ha representado el objeto de las mejoras.

DESCRIPCION DE LAS FIGURAS

FIG.1 muestra el dispositivo de aleatorización-encriptación que incluye la primer realización de las mejoras introducidas en la patente principal nº 9801037, siendo dichas mejoras objeto de la presente.

FIG.2 muestra el dispositivo de desencriptación correspondiente que incluye las mejoras necesarias para la desencriptación de secuencias aleatorizadas-encriptadas con el dispositivo de la FIG.1.

FIG.3 muestra la segunda realización del dispositivo de aleatorización-encriptación objeto la patente principal nº 9801037, que incluye la primer realización de las mejoras introducidas.

FIG.4 muestra el dispositivo de desencriptación correspondiente que incluye las mejoras necesarias para la desencriptación de secuencias aleatorizadas-encriptadas con el dispositivo de la FIG.3.

FIG.5 muestra la segunda realización de las mejoras aplicadas en el dispositivo de aleatorización-encriptación con las modificaciones aplicadas con respecto al dispositivo de la FIG.1.

FIG.6 muestra el dispositivo de desencriptación correspondiente que incluye las mejoras necesarias para la desencriptación de secuencias aleatorizadas-encriptadas con el dispositivo de la FIG.5.

FIG.7 muestra segunda realización de las mejoras aplicadas en el dispositivo de aleatorización-encriptación con las modificaciones aplicadas con respecto al dispositivo de la FIG.3.

FIG.8 muestra el dispositivo de desencriptación correspondiente que incluye las mejoras necesarias para la desencriptación de secuencias aleatorizadas-encriptadas con el dispositivo de la FIG.7.

MODOS DE REALIZACION

En la presente exposición de modos de realización de las mejoras de la patente principal nº 9801037 por "dispositivo de aleatorización-encriptación de secuencia de datos", partes correspondientes a partes de las FIG.1, FIG.2, FIG.3, FIG.4, FIG.5, FIG.6, FIG.7, FIG.8 y FIG.9 de la referida patente principal son designadas por mismas referencias alfanuméricas con el objeto de facilitar la comprensión del modo en que se integran dichas mejoras. Asimismo, las referencias realizadas a elementos de la descripción de la patente estadounidense número 5,214,703, de título "Device for the conversion of a digital block and use of same" del 25 de Mayo de 1993, tales como unidades de generación de subbloques clave (referencias 202 y 401 de la patente principal nº 9801037), bloque clave o bloque de control Z, subbloques clave Z_1 a Z_{52}, subbloques clave U_1 a U_{52}, siguen las pautas de la patente principal nº 9801037 con el objetivo de facilitar el conocimiento de los elementos objeto que son referenciados.

FIG.1 muestra diagrama básico de enlazado de bloques del dispositivo para aleatorización-encriptación de un mensaje de texto claro con la primer realización de las mejoras incorporadas. En la FIG.1, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.6 de la patente principal son designadas por mismas referencias alfanuméricas.

En esta variante de la unidad de aleatorización-encriptación 501v2, las mejoras se concretan por las substituciones de unidad divisora de bloque de control 601, unidad 602, entrada/salida 610, bloque de control Kp, bloque inicial de control W y bloque WI de la FIG.6 de la patente principal por unidad divisora de bloque de control 1001, unidad generadora de bloque transformador 1002, entrada/salida 1010, bloque de control Kpv2, bloque inicial de control R y bloque transformador WTI respectivamente.

A continuación se describen las mencionadas mejoras incorporadas.

La unidad divisora de bloque de control 1001, presenta entrada 107 y salidas 611 y 1010, salida 611 formada por 128 líneas paralelas y salida 1010 formada por G líneas paralelas. La unidad divisora de bloque de control 1001 recibe la clave de aleatorización-encriptación o bloque de control Kpv2 por canal 107, dividiendo el

bloque de control Kpv2 en dos bloques iniciales de control Z y R. Siendo el bloque inicial de control Z de longitud preferentemente L1=128 bits, y el bloque inicial de control R de longitud preferentemente L3=G bits. El bloque inicial de control Z se suministra a la unidad de generación de subbloques de control 202 por salida 611, la unidad de generación de subbloques de control 202 genera subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, que se suministran por entrada secundaria 311 de la unidad de encriptación-desencriptación 204. El subbloque inicial de control R se suministra a la unidad generadora de bloque transformador 1002 por salida 1010.

La unidad generadora de bloque transformador 1002, presenta entrada 1010, formada por G lineas paralelas, y entrada 614 y salida 613, formada cada una de ellas por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 1002 suministrar el bloque transformador WTI de longitud N=64 bits que se da como entrada de la unidad de agrupación 603 por entrada 613.

La unidad generadora de bloque transformador 1002 implementa función F, tal que genera el bloque transformador WTI a partir del bloque inicial de control R y el bloque de texto aleatorizado-encriptado de salida YI resultado de la aleatorización-encriptación del anterior bloque de texto claro XI. El bloque transformador WTI va adquiriendo los siguientes valores mostrados en la TABLA 1 para los diferentes y sucesivos bloques de texto claro XI ensamblados de un texto claro $\underline{X}$ que es aleatorizado-encriptado; siendo el bloque de texto aleatorizado-encriptado de salida YI_1 el resultado de la aleatorización-encriptación del primer bloque de texto claro XI_1, el bloque de texto aleatorizado-encriptado de salida YI_2 el resultado de la aleatorización-encriptación del segundo bloque de texto claro XI_2, y así sucesivamente.

TABLA 1
VALORES QUE ADQUIERE WTI

Orden de bloque de texto claro que es aleatorizado-encriptado	Bloque de texto claro que es aleatorizado-encriptado	Bloque que contiene WTI
Primero	XI_1	F(R)
Segundo	XI_2	F(YI_1)
Tercero	XI_3	F(YI_2)
....	.....	....
N	XI_n	F(YI_{n-1})

La función F implementada en la unidad generadora de bloque transformador

1002 podría ser definida entre múltiples maneras como:

- $WTI_1 = F(R) = H_1(R)$, para el primer bloque WTI
- $WTI_n = F(YI_{n-1}) = H_n(R, YI_{n-1})$, para el "enésimo" bloque WTI que se genera para la aleatorización-encriptación del "enésimo" bloque de texto claro XI

Donde:

- $WTI_1 = H_1(R)$ podría ser:

  bloque WTI = R, la identidad, o

  bloque WTI resultado de cálculos realizados con R, por ejemplo.

y

- $WTI_n = H_n(R, YI_{n-1})$ entre muchas posibles implementaciones:
  - Podría ser $H_n(R, YI_{n-1}) = E_n(R)$ oper1 YI_{n-1}:

    Donde oper1 puede ser la operación XOR u Or-exclusiva.

    Y $E_n(R)$ podría elegirse para que implementase una de las funciones que se exponen a continuación, por exponer algunas de las posibles y sin que se tenga que limitar a las mismas, como son:

    - $E_n(R) = (E_{n-1}(R) + 1) \bmod 2^{64}$.
    - Dividido el bloque R en dos subbloques R1 y R2 de longitud de 32 bits cada uno puede implementarse como $E_n(Ri) = (E_{n-1}(Ri) + 1) \bmod 2^{32}$ para i=1,2.
    - $E_n(R) = (E_{n-1}(R) - 1) \bmod 2^{64}$.
    - Dividido el bloque R en dos subbloques R1 y R2 de longitud de 32 bits cada uno puede implementarse como $E_n(Ri) = (E_{n-1}(Ri) - 1) \bmod 2^{32}$ para i=1,2.
    - En general, dividido el bloque R en Q subbloques, siendo Q divisor de 64, R1, ... RQ de longitud de 64/Q bits cada uno puede implementarse como $E_n(Ri) = (E_{n-1}(Ri)$ oper2 $B) \bmod 2^{64/Q}$ para i=1,...,Q, donde B es un valor, y oper2 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.
    - U otra implementación general, dividido el bloque R en diferentes subbloques R1,..., RD, tales que Ri formado por longitud de Qi bits, siendo Qi menor o igual a 64, $E_n(Ri) = (E_{n-1}(Ri)$ oper2 $B) \bmod 2^{Qi}$ para i=1,...,D, donde B es un valor, y oper2 puede ser la adición o la

sustracción por ejemplo, sin limitar otras posibles operaciones.

Siendo definida la función "mod" previa como la operación "módulo" tal como se conoce en el arte, tal que "a = b mod c" donde "a" es el resto de la división entera de "b" por "c".

En estas seis implementaciones específicas previamente mostradas el bloque inicial de control R es preferentemente de longitud G=64 bits recibido por entrada 1010, de 64 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 192 bits.

- E_n (R) ser adaptación de generador de números aleatorios, como el aparecido originalmente en "Toward a Universal Random Number Generator", autor George Marsaglia y Arif Zaman, Florida State University de U.S.A., Report: FSU-SCRI-87-50 (1987), el cual a partir del bloque de control R que le es suministrado como lo que los entendidos en el arte entienden por "seed", puede ir generando bloques de 64 bits de datos aleatorios a ser utilizados como función E_n. Haciendo uso el generador de una "seed" de 32 bits en este caso particular de generador de números aleatorios, el bloque inicial de control R es preferentemente de longitud G=32 bits recibido por entrada 1010, de 32 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 160 bits.

- E_n (R) hacer uso de función de hash MD5, descrita en "Request for Comments: 1321" o "rfc1321", autor R.Rivest, del MIT Laboratory for Computer Science and RSA Data Security, Inc., U.S.A., del Abril de 1992, la cual a partir del bloque de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits a ser utilizados como función E_n de modo que E_n (R) = 64 bits seleccionados de $MD5_n$ (R) y $MD5_n$ (R) = MD5 ($MD5_{n-1}$ (R)) por ejemplo. Por las características de las funciones de hash, el bloque inicial de control R puede ser de cualquier longitud G, y por lo tanto el bloque de control Kpv2 es preferentemente de 128 + G bits en este caso.

- E_n (R) hacer uso de función de hash SHA1, objeto de la publicación "Federal Information Processing Standards Publication 180-1" o "FIPS PUB 180-1" del 17 de Abril de 1995, que anuncia el "Secure Hash Standard", del "National Institute of Standards and Technology" ("NIST")

del Departamento de Comercio del Gobierno de los Estados Unidos. La cual a partir del bloque de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits a ser utilizados como función E_n de modo que E_n (R) = 64 bits seleccionados de $SHA1_n$ (R) y $SHA1_n$ (R) = SHA1 ($SHA1_{n-1}$ (R)) por ejemplo. Al igual que en el caso previo referente a la función de hash MD5, el bloque inicial de control R puede ser de cualquier longitud G, y por lo tanto el bloque de control Kpv2 es preferentemente de 128 + G bits en este caso.

- Otras posibles implementaciones de E_n (R).

- Podría ser H_n(R , YI_{n-1}) = R oper1 E'_n (YI_{n-1}):

  Donde oper1 puede ser también la operación XOR u Or-exclusiva.

  Y E'_n (YI_{n-1}) podría ser una entre las siguientes, y sin tener que limitarse a las mismas:

  - E'_n (YI_{n-1}) = (YI_{n-1} + 1) mod 2^{64} .
  - Dividido el bloque YI_{n-1} en dos subbloques $YI_{n-1}1$ y $YI_{n-1}2$ de longitud de 32 bits cada uno puede implementarse como E'_n ($YI_{n-1}i$) = ($YI_{n-1}i$ + 1) mod 2^{32} para i=1,2.
  - E'_n (YI_{n-1}) = (YI_{n-1} - 1) mod 2^{64} .
  - Dividido el bloque YI_{n-1} en dos subbloques $YI_{n-1}1$ y $YI_{n-1}2$ de longitud de 32 bits cada uno puede implementarse como E'_n ($YI_{n-1}i$) = ($YI_{n-1}i$ - 1) mod 2^{32} para i=1,2.
  - En general, dividido el bloque YI_{n-1} en Q subbloques, siendo Q divisor de 64, $YI_{n-1}1$, ... ,$YI_{n-1}Q$ de longitud de 64/Q bits cada uno puede implementarse como E'_n ($YI_{n-1}i$) = ($YI_{n-1}i$ oper2 B) mod $2^{64/Q}$ para i=1,...,Q, donde B es un valor, y oper2 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.
  - O igualmente, otra implementación general, dividido el bloque R en diferentes subbloques R1,..., RD, tales que Ri formado por longitud de Qi bits, siendo Qi menor o igual a 64, E'_n (Ri) = (E'_{n-1} (Ri) oper2 B) mod 2^{Qi} para i=1,...,D, donde B es un valor, y oper2 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

  Siendo la función "mod" la operación previamente descrita.

  - Hacer uso de función de hash como MD5 o SHA1, ya mencionadas

previamente, tal que $E'_n(YI_{n-1}) = 64$ bits seleccionados de MD5 (YI_{n-1}) o 64 bits seleccionados de SHA1 (YI_{n-1}).

En estas implementaciones específicas previamente mostradas el bloque inicial de control R es preferentemente de longitud G=64 bits recibido por entrada 1010, de 64 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 192 bits.

- Otras posibles implementaciones de $E'_n(YI_{n-1})$.

- Podría ser $H_n(R , YI_{n-1}) = YI_{n-1}$ oper3 $H_{n-1}(R, YI_{n-2})$ donde por ejemplo:
  - oper3 puede ser también la operación XOR u Or-exclusiva.
  - y $H_1(R, YI_0) = R$.

  En esta implementación específica el bloque inicial de control R es preferentemente de longitud G=64 bits recibido por entrada 1010, de 64 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 192 bits.
- Otras posibles implementaciones de $WTI_n = F (YI_{n-1}) = H_n (R , YI_{n-1})$.

Obviamente existen y existirán implementaciones de la función F específicas, implementada en la unidad generadora de bloque transformador 1002, que presentan más alta probabilidad que otras funciones F de que el dispositivo de aleatorización-encriptación resultado de incorporar las mejoras produzca texto aleatorizado-encriptado que cumpla con los tests de aleatoriedad implementados en el analizador de aleatoriedad 503 de la FIG.5 de la patente principal en función del texto claro X que se desee aleatorizar-encriptar con una clave de encriptación o bloque de control Kpv2. Cabe mencionar, que en el caso particular que $WTI = H_1(R) = R$ y que $WTI = H_n (R , YI_{n-1}) = YI_{n-1}$ nos encontraríamos que tendríamos el dispositivo objeto de la patente principal descrito en el primer modo de realización de la misma.

Las ventajas que se obtienen con la introducción de las mejoras se concretan en la agrupación del bloque de texto claro XI con un bloque transformador WTI no accesible por ataques criptoanalíticos y, en función de la implementación particular que se realice de la función F, no deducible; y en que el bloque de control Kpv2 puede tener una longitud superior a la que tiene el dispositivo objeto de la patente principal nº 9801037. La longitud del bloque de control Kpv2 puede ser preferentemente de longitud suma de la longitud del bloque inicial de control Z, preferentemente de 128 bits, y la longitud del bloque inicial de control R, el cual tendrá preferentemente la

longitud del bloque inicial de la unidad generadora de bloque transformador 1002, aunque es dependiente de la implementación particular que se realice de esta última. En el caso particular de que la unidad generadora de bloque transformador 1002 implemente la función E_n (Ri) = (E_{n-1} (Ri) + B) mod $2^{64/Q}$ para subbloques R1 a RQ, el bloque inicial de control R es preferentemente de 64 bits, con lo que el bloque de control Kpv2 es preferentemente de 192 bits, caso en el que no se consigue ventaja respecto a la longitud del bloque de control del dispositivo objeto de la patente principal; en el caso de que haga uso de la función de hash SHA1 puede definirse como preferentemente el bloque inicial de control R de 160 bits, con lo que el bloque de control Kpv2 es preferentemente de 288 bits; etcétera. Se tiene más seguridad en la confidencialidad de la información aleatorizada-encriptada, pues cuanto mayor sea la longitud del bloque de control Kpv2 mayor es la seguridad que se puede tener ante ataques enemigos al verse incrementado el coste de los ataques por fuerza bruta que pueden llevarse a cabo.

En lo que sigue se realiza una exposición del resto del dispositivo con las mejoras previamente expuestas incorporadas con el objeto de clarificar la integración de las mismas en el dispositivo objeto de la patente principal. Con la incorporación de las mejoras se tiene que el texto claro $\underline{X}$ a ser aleatorizado-encriptado llega continuamente de la fuente de mensajes 101 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto claro XI de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 612, que es entrada de unidad de agrupación 603. La unidad de agrupación 603 presenta dos entradas 612 y 613, de 64 líneas paralelas cada una, y salida 312, también de 64 líneas paralelas. En la unidad de agrupación 603 se agrupan los bloques XI y WTI, ambos de longitud N=64 bits que llegan por entradas 612 y 613 respectivamente, generando un interbloque VI de longitud N=64 bits.

La operación de agrupación que se realiza en la unidad de agrupación 603 es la OR-exclusiva o-XOR bit a bit, de tal modo que XI $\oplus$ WTI $\rightarrow$ VI.

Este interbloque VI alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta unidad de encriptación-desencriptación 204, el interbloque VI es agrupado junto con los cincuenta y dos subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, generados por la

unidad de generación de subbloques de control 202 y que llegan por segunda entrada 311.

Finalmente, un bloque de texto aleatorizado-encriptado de salida YI de longitud N=64 bits, aparece en la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313, formada por 64 líneas paralelas, está conectada a la unidad de salida 302 y por entrada 614 a la unidad generadora de bloque transformador 1002. La entrada 614 tiene como una de múltiples implementaciónes, el ser una derivación de la salida 313. El bloque de texto aleatorizado-encriptado de salida YI por la salida 313 alcanza la unidad de salida 302 y también el mismo bloque de texto aleatorizado-encriptado YI se suministra a la unidad generadora de bloque transformador 1002 por entrada 614 para ser utilizado en la generación por la unidad generadora de bloque transformador 1002 del bloque transformador WTI a ser utilizado en la aleatorización-encriptación del siguiente bloque de texto claro XI que será ensamblado en la unidad ensambladora de entrada 301 en el siguiente paso de aleatorización-encriptación.

Este bloque de texto aleatorizado-encriptado YI puede ser convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 505. Todos los bloques de texto aleatorizado-encriptado YI juntos forman el texto aleatorizado-encriptado Yp.

Al igual que con el dispositivo objeto de la patente principal, el dispositivo de la FIG.1 genera a partir de la secuencia de texto claro X, que se suministra como entrada, texto aleatorizado-encriptado Yp de salida, el cual presenta substancialmente características propias de las secuencias aleatorias verificables en el analizador de aleatoriedad 503 de la FIG.5 de la patente principal, permitiendo evaluar si la clave de aleatorización-encriptación o bloque de control Kpv2 usada introduce la confusión y difusión deseada. Por lo tanto, al igual que los dispositivos de aleatorización-encriptación de las FIG.6 y FIG.8 de la patente principal el dispositivo de aleatorización-encriptación de la FIG.1 puede ser también utilizado como generador de secuencias de números aleatorios; suministrando diferentes datos de entrada como texto claro X una secuencia de números aleatoria es suministrada como salida Yp. Asimismo, también puede ser utilizable el dispositivo de la FIG.1, al igual que los dispositivos de las FIG.6 y FIG.8 de la patente principal, como lo que los entendidos en el arte de la encriptación entienden como "función de encriptación en una

dirección" o "one-way hash function".

Por la realimentación que se realiza a la unidad generadora de bloque transformador 1002 con el bloque de texto aleatorizado-encriptado de salida YI por medio de la entrada/salida 614 tenemos que un cambio en un bit del bloque de texto claro XI, implica cambios en todos los subsiguientes bloques de texto aleatorizado-encriptado YI, y por lo tanto cambios en la secuencia de texto aleatorizado-encriptado Yp resultado.

FIG.2 muestra diagrama básico de enlazado de bloques del dispositivo de desencriptación de un mensaje de texto aleatorizado-encriptado con el dispositivo de aleatorización-encriptación incorporando la primer realización de las mejoras mostrado en la FIG.1 de la presente memoria. En la FIG.2, partes correspondientes a partes de las FIG.1, FIG.4, FIG.5 y FIG.7 de la patente principal son designadas por mismas referencias alfanuméricas con objeto de facilitar las referencias.

En esta variante de la unidad de desencriptación 502v2, las mejoras se concretan en la substitución de unidad divisora de bloque de control 701, unidad 702, entrada/salida 710, bloque de control Ks, bloque inicial de control W y bloque WJ de la FIG.7 de la patente principal por unidad divisora de bloque de control 2001, unidad generadora de bloque transformador 2002, entrada/salida 2010, bloque seleccionado de control Ksv2, bloque inicial de control R y bloque transformador WTJ respectivamente.

Se facilita a continuación una descripción de las mejoras, y la integración de las mismas en el dispositivo.

La unidad divisora de bloque de control 2001, presenta entrada 108 y salidas 2010 y 711, salida 2010 formada por G líneas paralelas y salida 711 formada por 128 líneas paralelas. La unidad divisora de bloque de control 2001 recibe el bloque de clave o bloque seleccionado de control Ksv2 por canal 108, dividiendo el bloque seleccionado de control Ksv2 en dos bloques iniciales de control Z y R. La unidad divisora de bloque de control 2001 divide el bloque seleccionado de control Ksv2 de igual modo que la unidad divisora de bloque de control 1001 del dispositivo de la FIG.1 dividió el bloque seleccionado de control Ksv2 para la aleatorización-encriptación del mensaje de texto aleatorizado-encriptado Ys que es desencriptado. Siendo el bloque inicial de control Z de longitud preferentemente L1=128 bits, y el bloque inicial de control R de longitud preferentemente L3=G bits. El bloque inicial

de control Z se suministra a la unidad de generación de subbloques de control 401 por salida 711 para que la unidad de generación de subbloques de control 401 genere subbloques de control U_1 a U_{52}, de longitud M = 16 bits cada uno, que se suministran por entrada secundaria 311 a la unidad de encriptación-desencriptación 204. El bloque inicial de control R se suministra a la unidad generadora de bloque transformador 2002 por salida 2010.

La unidad generadora de bloque transformador 2002, presenta entrada 2010, formada por G lineas paralelas, y entrada 713 y salida 714, formada cada una de ellas por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 2002 suministrar el bloque transformador WTJ de longitud N=64 bits que se da como entrada de la unidad de agrupación 704 por entrada 714.

La unidad generadora de bloque transformador 2002 implementa función F generadora de bloque transformador WTJ igual a la función F específica que implementa la unidad generadora de bloque transformador 1002 del dispositivo de la FIG.1 con que se aleatorizó-encriptó el texto claro X con la clave de aleatorización-encriptación o bloque seleccionado de control Ksv2 que generó el texto aleatorizado-encriptado Ys objeto de la desencriptación en particular que se esté llevando a cabo.

La TABLA 2 muesta los diferentes valores que adquiere el bloque WTJ para los diferentes bloques de texto aleatorizado-encriptado YJ que es desencriptado.

TABLA 2
VALORES QUE ADQUIERE WTJ

Orden de bloque de texto aleatorizado-encriptado que es desencriptado	Bloque de texto aleatorizado-encriptado que es desencriptado	Bloque que contiene WTJ
Primero	YJ_1	F(R)
Segundo	YJ_2	F(YJ_1)
Tercero	YJ_3	F(YJ_2)
....	.....	....
N	YJ_n	F(YJ_{n-1})

El dispositivo de desencriptación muestra la necesidad del uso del bloque transformador WTJ generado en la unidad generadora de bloque transformador 2002 para poder llevar a cabo la desencriptación de la secuencia de texto Ys, siendo el bloque transformador WTJ no accesible y desconocido a diferencia del dispositivo objeto de la patente principal.

Se describe a continuación la interactuación del resto del dispositivo con las mejoras incorporadas. El texto aleatorizado-encriptado Ys a ser descifrado llega continuamente por el canal de transmisión 103 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto aleatorizado-encriptado YJ de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 312, formada por 64 líneas paralelas, que conecta con la unidad de encriptación-desencriptación 204, y con la unidad 702 por entrada 712. La entrada 712 de la unidad 702 puede ser una derivación de la salida 312 y está también formada por 64 líneas paralelas. Una vez ensamblado el bloque de texto aleatorizado-encriptado YJ se suministra a la unidad de encriptación-desencriptación 204 y a la unidad 702 por salida 312.

La unidad 702 presenta entrada 712 y salida 713, cada una formada por 64 líneas paralelas. El propósito de la unidad 702 es mantener una copia del actual bloque de texto aleatorizado-encriptado YJ que se suministra como entrada de la unidad de encriptación-desencriptación 204 para la utilización posterior por parte de la unidad generadora de bloque transformador 2002 descrita previamente.

El bloque de texto aleatorizado-encriptado YJ alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312. En esta unidad de encriptación-desencriptación 204, el bloque YJ es agrupado juntos con los cincuenta y dos subbloques de control U_1 a U_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 401 y llegan por segunda entrada 311 a la unidad de encriptación-desencriptación 204.

Tras la agrupación del bloque de texto YJ y los subbloques de control U_1 a U_{52} en la unidad de encriptación-desencriptación 204, un bloque de texto SJ de longitud N=64 bits aparece en salida 313 de la unidad de encriptación-desencriptación 204. La salida 313 esta formada por 64 líneas paralelas, y es entrada de la unidad de agrupación 704.

La unidad de agrupación 704 consta de entradas 313 y 714, y salida 715, de 64 líneas paralelas cada una. En esta unidad de agrupación 704 se agrupan los bloques SJ y WTJ, ambos de longitud N=64 bits que llegan por entradas 313 y 714 respectivamente, dando como salida un bloque de texto claro XJ de longitud N=64 bits. La operación de agrupación que se realiza en la unidad de agrupación 704 es la

conocida OR-exclusiva o XOR bit a bit de tal modo que SJ ⊕ WTJ → XJ.

Este bloque de texto claro XJ se suministra por salida 715, formada por 64 líneas paralelas, a la unidad de salida 302. Una vez se tiene el bloque de texto claro XJ, se suministra por entrada 713 el actual bloque de texto aleatorizado-encriptado YJ que contiene la unidad 702 a la unidad generadora de bloque de transformador 2002, para que en la desencriptación del siguiente bloque de texto aleatorizado-encriptado YJ que es ensamblado, la unidad generadora de bloque de transformador 2002 genere el bloque transformador WTJ que ha de ser utilizado. También es posible la eliminación de la unidad 702, si la unidad generadora de bloque de transformador 2002 se implementa de modo que puede recibir el actual bloque de texto aleatorizado-encriptado YJ y utilizarlo en la generación del bloque transformador WTJ que será usado en la desencriptación del siguiente bloque de texto aleatorizado-encriptado YJ; ello conllevaría así mismo la eliminación de la entrada/salida 713 y ser entrada de la unidad generadora de bloque de transformador 2002 la entrada 712. Se deja en la FIG. 2 la unidad 702 y la entrada/salida 713 por considerarlo más clarificador de la operativa.

El bloque de texto claro XJ es convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido a la unidad de destino 105, la cual obtiene el texto claro $\underline{X}$ tras realizarse todo el proceso con la secuencia $\underline{Ys}$.

Al final de la desencriptación con el dispositivo de desencriptación 502v2 del texto aleatorizado-encritpado $\underline{Ys}$ con la clave de desencriptación o bloque seleccionado de control Ksv2, se obtiene el texto claro $\underline{X}$ objeto de la aleatorización-encriptación con el dispositivo de aleatorización-encriptación 501v2 de la FIG.1 haciendo uso de la clave de aleatorización-encriptación o bloque seleccionado de control Ksv2.

FIG.3 muestra la segunda realización del dispositivo de aleatorización-encriptación objeto la patente principal nº 9801037 incluyendo la primer realización de las mejoras objeto de la presente invención. En la FIG.3, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.8 de la patente principal son designadas por mismas referencias alfanuméricas.

En esta variante de la unidad de aleatorización-encriptación 501v3, las mejoras

se concretan por las substituciones de unidad 602v y bloque WI de la FIG.8 de la patente principal por unidad generadora de bloque transformador 1002v y bloque transformador WTI respectivamente, así como introducción del bloque inicial de control R.

Se describe a continuación las mencionadas mejoras que son incorporadas.

La unidad generadora de bloque transformador 1002v, presenta entrada 614 y salida 613, formada cada una de ellas por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 1002v suministrar el bloque transformador WTI de longitud N=64 bits que se da como entrada de la unidad de agrupación 603 por entrada 613. La unidad generadora de bloque transformador 1002v genera el bloque transformador WTI con bloque inicial de control R y bloque de salida YI. El bloque inicial de control R de longitud preferentemente L3=G bits en esta realización está prefijado para la aleatorización-encriptación de una secuencia de texto claro X, no depende del bloque de control Kpv que se suministra por el canal 107 al dispositivo.

Para la generación del bloque transformador WTI la unidad generadora de bloque transformador 1002v implementa función F que hace uso del bloque inicial de control R y el bloque de texto aleatorizado-encriptado de salida YI resultado de la aleatorización-encriptación del anterior bloque de texto claro XI al igual que la unidad generadora de bloque transformador 1002 de la FIG.1. La función F que implementa la unidad generadora de bloque transformador 1002v puede ser idéntica a la función F expuesta previamente que implementa la unidad generadora de bloque transformador 1002 de la FIG.1, y ser cualquiera de las opciones que se han descrito para la misma con respecto a la unidad generadora de bloque transformador 1002 de la FIG.1; la diferencia estriba en que el bloque inicial de control R está prefijado en el dispositivo de la FIG.3, mientras que en el dispositivo de la FIG.1 es suministrado por la unidad divisora de bloque de control 1001.

En esta realización se consigue la ventaja referente al desconocimiento por parte de enemigos del bloque transformador WTI a ser agrupado en la unidad de agrupación 603 con el bloque de datos XI, pero no así la ventaja de usar una mayor longitud de bloque de control, pues, respecto a la realización de la patente principal, ésta no sufre cambios.

No se realiza la descripción del dispositivo resultante con las mejoras

incorporadas al considerarse que la similitud con la descripción ofrecida en el modo de realización del dispositivo de la FIG.1 y la propia FIG.3 permiten comprender cual es el modo de funcionamiento del mismo.

Al igual que en el dispositivo de la FIG.1, el dispositivo de la FIG.3 también puede ser usado como generador de números aleatorios, ya que suministrándole diferentes datos de entrada como secuencia de texto X, se obtiene una secuencia de números aleatorios como texto aleatorizado-encriptado de salida Yp. Asimismo, también es utilizable como "función de encriptación en una dirección" o función de hash, y por la realimentación que se realiza a la unidad generadora de bloque transformador 1002v con el bloque de texto aleatorizado-encriptado de salida YI por medio de la entrada/salida 614 tenemos que un cambio en un bit del bloque de texto claro XI, implica cambios en todos los subsiguientes bloques de texto aleatorizado-encriptado YI, y por lo tanto cambios en la secuencia de texto aleatorizado-encriptado Yp resultado.

FIG.4 muestra el dispositivo de desencriptación correspondiente al dispositivo de la FIG.3. En la FIG.4, partes correspondientes a partes de las FIG.1, FIG.4, FIG.5 y FIG.9 de la patente principal son designadas por mismas referencias alfanuméricas.

En esta variante de la unidad de desencriptación 502v3, las mejoras se concretan por las substituciones de unidad 703v y bloque WJ de la FIG.9 de la patente principal por unidad generadora de bloque transformador 2002v y bloque transformador WTJ respectivamente, así como introducción del bloque inicial de control R.

Se describe a continuación las mencionadas mejoras que son incorporadas.

La unidad generadora de bloque transformador 2002v, presenta entrada 713 y salida 714, formada cada una de ellas por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 2002v suministrar el bloque transformador WTJ de longitud N=64 bits que se da como entrada de la unidad de agrupación 704 por entrada 714. La unidad generadora de bloque transformador 2002v genera el bloque transformador WTJ con bloque inicial de control R y bloque de datos YJ. El bloque inicial de control R de longitud preferentemente L3=G bits en esta realización está prefijado para la desencriptación de la secuencia de texto aleatorizado-encriptado Ys, no depende del bloque de control Ksv que se suministra al dispositivo por el canal 107, y debe ser igual al bloque inicial de control R utilizado en el dispositivo de la FIG.3 con que se aleatorizó-encriptó la secuencia de texto

aleatorizado-encriptado Ys objeto de la desencriptación actual.

La unidad generadora de bloque transformador 2002v implementa función F, tal que genera el bloque transformador WTJ a partir del bloque inicial de control R y el bloque de datos YJ previamente desencriptado, al igual que la unidad generadora de bloque transformador 2002 de la FIG.2. La función F específica que implementa la unidad generadora de bloque transformador 2002v es igual a la función F específica implementada en la unidad generadora de bloque transformador 1002v del dispositivo de la FIG.3 con que se aleatorizó-encriptó la secuencia de texto aleatorizado-encriptado Ys objeto de la desencriptación actual.

Al igual que en el dispositivo de la FIG.2 también es posible la eliminación de la unidad 702, si la unidad generadora de bloque de transformador 2002v se implementa de modo que puede recibir el actual bloque de texto aleatorizado-encriptado YJ y utilizarlo en la generación del bloque transformador WTJ que será usado en la desencriptación del siguiente bloque de texto aleatorizado-encriptado YJ que será ensamblado; ello conllevaría asimismo la eliminación de la entrada/salida 713 y ser entrada de la unidad generadora de bloque de transformador 2002v la entrada 712. Se deja en la FIG. 4 la unidad 702 y la entrada/salida 713 por considerarlo más clarificador de la operativa.

El dispositivo de la FIG.4 también permite ver la necesidad de usar el bloque transformador WTJ para la desencriptación de la secuencia de texto aleatorizada-encriptada Ys y comprender la ventaja que comporta ante ataques enemigos.

No se realiza la descripción del dispositivo resultante con las mejoras incorporadas al considerarse que la similitud con la descripción ofrecida en el modo de realización de la FIG.2 y la propia FIG.4 permiten comprender cual es el modo de funcionamiento del mismo.

FIG.5 muestra diagrama básico de enlazado de bloques de la segunda realización de las mejoras en la primer realización del dispositivo de aleatorización-encriptación de una secuencia de texto claro objeto de la patente principal nº 9801037. En la FIG.5, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.6 de la patente principal, y FIG.1 de la presente memoria son designadas por mismas referencias alfanuméricas con objeto de facilitar las referencias.

Con respecto a la FIG.1 de la presente memoria, la cual presenta la primer realización de las mejoras, en esta variante de la unidad de aleatorización-encriptación

501v4, la segunda realización de las mejoras se concretan en la substitución adicional de unidad generadora de bloque transformador 1002 y bloque transformador WTI por unidad generadora de bloque transformador 5002 y bloque transformador WTIv respectivamente, y eliminación adicional de entrada/salida 614.

Se describe a continuación dicha segunda realización de las mejoras.

La unidad divisora de bloque de control 1001 presenta entrada 107 y salidas 611 y 1010, salida 611 formada por 128 líneas paralelas y salida 1010 formada por G líneas paralelas. La unidad divisora de bloque de control 1001 recibe la clave de aleatorización-encriptación o bloque de control Kpv2 por canal 107 y divide el bloque de control Kpv2 en dos bloques iniciales de control Z y R. Siendo el bloque inicial de control Z de longitud preferentemente L1=128 bits, y el bloque inicial de control R de longitud preferentemente L3=G bits. El bloque inicial de control Z se suministra a unidad de generación de subbloques de control 202 por salida 611. El subbloque inicial de control R se suministra a la unidad generadora de bloque transformador 5002 por salida 1010. La unidad generadora de bloque transformador 5002, presenta entrada 1010, formada por G lineas paralelas, y salida 613, formada por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 5002 suministrar el bloque WTIv de longitud N=64 bits que se da como entrada de la unidad de agrupación 603 por entrada 613.

La unidad generadora de bloque transformador 5002 implementa función F', tal que el bloque WTIv va adquiriendo los siguientes valores mostrados en la TABLA 3 para los diferentes y sucesivos bloques de texto claro XI de un texto claro X que es aleatorizado-encriptado.

TABLA 3
VALORES QUE ADQUIERE WTIv

Orden de bloque de texto claro que es aleatorizado-encriptado	Bloque de texto claro que es aleatorizado-encriptado	Bloque que contiene WTIv
Primero	XI_1	$F'_1(R)$
Segundo	XI_2	$F'_2(R)$
Tercero	XI_3	$F'_3(R)$
....	.....	....
N	XI_n	$F'_n(R)$

La función F' implementada en la unidad generadora de bloque transformador 5002 puede ser definida entre múltiples maneras como:

- $WTIv_1 = F'_1(R)$, para el primer bloque WTIv
- $WTIv_n = F'_n(R)$, para el "enésimo" bloque WTIv que se genera para la aleatorización-encriptación del "enésimo" bloque de texto claro XI

Donde:

- $WTIv_1 = F'_1(R)$ puede ser:

  bloque WTIv = R, la identidad, o

  bloque WTIv resultado de cálculos realizados con R, por ejemplo.

y

- $WTIv_n = F'_n(R)$ puede ser, alguna entre las siguientes implementaciones, y sin tener que limitarse a las mismas:

  - $F'_n(R) = (F'_{n-1} (R) + 1) \bmod 2^{64}$.
  - Dividido el bloque R en dos subbloques R1 y R2 de longitud de 32 bits cada uno puede implementarse como $F'_n (Ri) = (F'_{n-1} (Ri) + 1) \bmod 2^{32}$ para i=1,2.
  - $F'_n(R) = (F'_{n-1} (R) - 1) \bmod 2^{64}$.
  - Dividido el bloque R en dos subbloques R1 y R2 de longitud de 32 bits cada uno puede implementarse como $F'_n (Ri) = (F'_{n-1} (Ri) - 1) \bmod 2^{32}$ para i=1,2.
  - En general, dividido el bloque R en Q subbloques, siendo Q divisor de 64, R1, ... RQ de longitud de 64/Q bits cada uno, puede implementarse como $F'_n (Ri) = (F'_{n-1} (Ri)$ oper2 B) $\bmod 2^{64/Q}$ para i=1,..,Q, donde B es un valor, y oper2 puede ser la adición o la sustracción por ejemplo y sin limitar otras posibles operaciones.
  - Otra posible implementación general, dividido el bloque R en diferentes subbloques R1,..., RD, tales que Ri formado por longitud de Qi bits, siendo Qi menor o igual a 64, $F'_n (Ri) = (F'_{n-1} (Ri)$ oper2 B) $\bmod 2^{Qi}$ para i=1,...,D, donde B es un valor, y oper2 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

  En estas seis implementaciones específicas previamente mostradas el bloque inicial de control R es preferentemente de longitud G=64 bits recibido por entrada 1010, de 64 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 192 bits.

  - $F'_n(R)$ hacer uso de adaptación de generador de números aleatorios,

como el anteriormente mencionado, aparecido originalmente en "Toward a Universal Random Number Generator", autor George Marsaglia y Arif Zaman, Florida State University Report: FSU-SCRI-87-50 (1987), el cual a partir del bloque de control R que le es suministrado como lo que los entendidos en el arte entienden por "seed", puede ir generando bloques de 64 bits aleatorios a ser utilizados como función F'. Haciendo uso el generador de una "seed" de 32 bits en este caso particular de generador de números aleatorios, el bloque inicial de control R es preferentemente de longitud G=32 bits recibido por entrada 1010, de 32 lineas paralelas, y por lo tanto el bloque de control Kpv2 es preferentemente de 160 bits.

- F'_n (R) hacer uso de función de hash MD5, la cual a partir del bloque de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits, de modo que F'_n (R) = 64 bits seleccionados de $MD5_n$ (R) y $MD5_n$ (R) = MD5 ($MD5_{n-1}$ (R)) por ejemplo. Por las características de las funciones de hash, el bloque inicial de control R puede ser de cualquier longitud G, y por lo tanto el bloque de control Kpv2 es preferentemente de 128 + G bits en este caso.

- F'_n (R) hacer uso de función de hash SHA1, la cual a partir del bloque de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits de modo que F'_m (R) = 64 bits seleccionados de $SHA1_n$ (R) y $SHA1_m$ (R) = SHA1 ($SHA1_{m-1}$ (R)) por ejemplo. Al igual que en el caso previo referente a la función de hash MD5, el bloque inicial de control R puede ser de cualquier longitud G, y por lo tanto el bloque de control Kpv2 es preferentemente de 128 + G bits en este caso.

- Otras posibles implementaciones.

Al igual que con la primer realización de las mejoras incorporadas en el dispositivo de aleatorización-encriptación de la FIG.1, existen y existirán implementaciones de la función F' específicas, implementada en la unidad generadora de bloque transformador 5002, que presentan más alta probabilidad que otras funciones F' de que el dispositivo con esta segunda realización de las mejoras genere texto aleatorizado-encriptado que cumpla con los tests de aleatoriedad implementados en el analizador de aleatoriedad 503 de la FIG.5 de la patente principal en función del

texto claro $\underline{X}$ que se desee aleatorizar-encriptar con una clave de encriptación Kpv2.

Al igual que con la primer realización de las mejoras, con esta segunda realización de las mejoras se tiene que el bloque de datos XI es agrupado en la unidad de agrupación 603 con un bloque transformador WTIv desconocido y no accesible, teniéndose además que el bloque de control Kpv2 puede ser preferentemente de longitud suma de la longitud del bloque inicial de control Z, preferentemente de 128 bits, y la longitud del bloque inicial de control R, el cual tendrá preferentemente la longitud del bloque inicial de la unidad generadora de bloque transformador 5002, y por tanto dependiente de la implementación particular que se realice de ésta última. En el caso de que la unidad generadora de bloque transformador implemente la función $F'_n (Ri) = (F'_{n-1} (Ri) + B) \bmod 2^{64/Q}$ para subbloques R1 a RQ, el bloque inicial de control R es preferentemente de 64 bits, con lo que el bloque de control Kpv2 es preferentemente de 192 bits, no siendo ventaja respecto al dispositivo de la patente principal; y en el caso de que haga uso de la función de hash SHA1 puede definirse el bloque inicial de control R de longitud preferentemente de 160 bits, con lo que el bloque de control Kpv2 es preferentemente de 288 bits; etcétera. Se tiene más seguridad en la confidencialidad de la información aleatorizada-encriptada, pues cuanto mayor sea la longitud del bloque de control Kpv2 mayor es la seguridad que se puede tener ante ataques enemigos al incrementar el coste de los ataques por fuerza bruta que se pueden realizar.

A continuación, con el objeto de facilitar la comprensión de la integración de esta segunda realización de las mejoras en el dispositivo de la patente principal nº 9801037, se pasa a realizar la exposición del mismo con las mejoras integradas. El texto claro $\underline{X}$ a ser cifrado llega continuamente de la fuente de mensajes 101 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto claro XI de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 612, que es entrada de unidad de agrupación 603. La unidad de agrupación 603 presenta dos entradas 612 y 613, de 64 líneas paralelas cada una, y salida 312, también de 64 líneas paralelas. En la unidad de agrupación 603 se agrupan los bloques XI y WTIv, ambos de longitud N=64 bits que llegan por entradas 612 y 613 respectivamente, generando un interbloque VI de longitud N=64 bits.

La operación de agrupación que se realiza en la unidad de agrupación 603 es la OR-exclusiva o XOR bit a bit, de tal modo que XI ⊕ WTIv → VI.

Este interbloque VI alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta unidad de encriptación-desencriptación 204, el interbloque VI es agrupado junto con los cincuenta y dos subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 202 y que llegan por segunda entrada 311.

Finalmente, un bloque de texto aleatorizado-encriptado de salida YI de longitud N=64 bits, aparece en la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313, formada por 64 líneas paralelas, está conectada a la unidad de salida 302. El bloque de texto aleatorizado-encriptado de salida YI por la salida 313 alcanza la unidad de salida 302.

Este bloque de texto aleatorizado-encriptado de salida YI puede ser convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 505. Todos los bloques de texto aleatorizado-encriptado de salida YI juntos forman el texto aleatorizado-encriptado Yp.

El dispositivo de la FIG.5 genera a partir de la secuencia de texto claro X, que se suministra como entrada, texto aleatorizado-encriptado Yp de salida, el cual presenta substancialmente características propias de las secuencias aleatorias, con lo que se puede medir objetivamente la confusión y difusión introducida en el mismo por la clave de encriptación o bloque de control Kpv2 utilizada. Por lo tanto, al igual que los dispositivos de aleatorización-encriptación de las FIG.6 y FIG.8 de la patente principal y FIG.1 y FIG.3 de la presente memoria, el dispositivo de aleatorización-encriptación de la FIG.5 puede ser también utilizado como generador de secuencias de números aleatorios; suministrando diferentes datos de entrada como texto claro X una secuencia de números aleatoria es sumnistrada como salida Yp.

FIG.6 muestra diagrama básico de enlazado de bloques de variante del dispositivo de desencriptación necesario para la desencriptación de un mensaje de texto aleatorizado-encriptado con el dispositivo de aleatorización-encriptación con las mejoras incorporadas mostrado en la FIG.5 de la presente memoria. En la FIG.6,

partes correspondientes a partes de las FIG.1, FIG.4, FIG.5 y FIG.7 de la patente principal y FIG.2 de la presente memoria son designadas por mismas referencias alfanuméricas.

En esta variante de la unidad de desencriptación 502v4, respecto a la FIG.2 de la presente memoria, la unidad generadora de bloque transformador 2002 y bloque transformador WTJ son substituidos por unidad generadora de bloque transformador 6002 y bloque transformador WTJv respectivamtente, y se eliminan entrada/salida 712 y 713, así como la unidad 702.

En lo que sigue se realiza una exposición de la segunda realización de las mejoras en dispositivo de desencriptación según la FIG.6.

La unidad divisora de bloque de control 2001 presenta entrada 108 y salidas 711 y 2010, salida 711 formada por 128 líneas paralelas y salida 2010 formada por G líneas paralelas. La unidad divisora de bloque de control 2001 recibe la clave de aleatorización-encriptación o bloque seleccionado de control Ksv2 por canal 108, y divide el bloque seleccionado de control Ksv2 en dos bloques iniciales de control Z y R. La unidad divisora de bloque de control 2001 divide el bloque de control Ksv2 del mismo modo al que la unidad divisora de bloque de control 1001 del dispositivo de la FIG.5 dividió el bloque seleccionado de control Ksv2 para la aleatorización-encriptación del mensaje de texto aleatorizado-encriptado Ys que es desencriptado, siendo el bloque inicial de control Z de longitud preferentemente L1=128 bits, y el bloque inicial de control R de longitud preferentemente L3=G bits. El bloque inicial de control Z se suministra a la unidad de generación de subbloques de control 401 por salida 711. El bloque inicial de control R se suministra a la unidad generadora de bloque transformador 6002 por salida 2010.

La unidad generadora de bloque transformador 6002, presenta entrada 2010, formada por G lineas paralelas, y salida 714, formada por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 6002 suministrar el bloque transformador WTJv de longitud N=64 bits que se da como entrada de la unidad de agrupación 704 por entrada 714.

La unidad generadora de bloque transformador 6002 implementa función F', que es la misma función, y por lo tanto la unidad es igual, a la función F' que implementa la unidad generadora de bloque transformador 5002 del dispositivo de la FIG.5 con que se aleatorizó-encriptó el texto claro X con la clave de aleatorización-

encriptación o bloque seleccionado de control Ksv2 dando el texto aleatorizado-encriptado Ys objeto de la desencriptación en particular que se esté llevando a cabo.

La TABLA 4 muesta los diferentes valores que adquiere el bloque WTJv para los diferentes bloques de texto aleatorizado-encriptado YJ que es desencriptado.

TABLA 4
VALORES QUE ADQUIERE WTJv

Orden de bloque de texto aleatorizado-encriptado que es desencriptado	Bloque de texto aleatorizado-encriptado que es desencriptado	Bloque que contiene WTJv
Primero	YJ_1	$F'_1(R)$
Segundo	YJ_2	$F'_2(R)$
Tercero	YJ_3	$F'_3(R)$
....	.....	....
N	YJ_n	$F'_n(R)$

Al igual que en las anteriores realizaciones de las mejoras, el dispositivo de la FIG.6 muestra la necesidad del uso del bloque transformador WTJv para poder realizar la desencriptación de la secuencia de texto aleatorizada-encriptada Ys, bloque transformador WTJv que al no ser accesible ni conocido hace más difíciles los ataques para descubrir la secuencia de texto claro X, o la clave de aleatorización-encriptación o bloque seleccionado de control Ksv2 usada.

A continuación se procede a describir el resto del dispositivo 502v4 de la FIG6 con el objeto de facilitar la comprensión del mismo y la integración de las mejoras. El texto aleatorizado-encriptado Ys a ser descifrado llega continuamente por el canal de transmisión 103 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto aleatorizado-encriptado YJ de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 312, formada por 64 líneas paralelas, que conecta con la unidad de encriptación-desencriptación 204. Una vez ensamblado el bloque de texto aleatorizado-encriptado YJ se suministra a la unidad de encriptación-desencriptación 204 por salida 312.

En esta unidad de encriptación-desencriptación 204, el bloque de texto aleatorizado-encriptado YJ es agrupado juntos con los cincuenta y dos subbloques de control U_1 a U_{52}, de longitud M=16 bits cada uno, generados por la unidad de

generación de subbloques de control 401 que llegan por segunda entrada 311 a la unidad de encriptación-desencriptación 204.

Tras la agrupación del bloque de texto aleatorizado-encriptado YJ y los subbloques de control U_1 a U_{52} en la unidad de encriptación-desencriptación 204, un bloque de texto SJ de longitud N=64 bits aparece en salida 313 de la unidad de encriptación-desencriptación 204. La salida 313 esta formada por 64 líneas paralelas, y es entrada de la unidad de agrupación 704.

La unidad de agrupación 704 consta de entradas 313 y 714, y salida 715, de 64 líneas paralelas cada una. En esta unidad de agrupación 704 se agrupan el bloque SJ y el bloque transformador WTJv, generado en la unidad de generación de bloque de transformación 6002 para la desencriptación del actual bloque de texto aleatorizado-encriptado YJ, ambos de longitud N=64 bits que llegan por entradas 313 y 714 respectivamente, dando como salida un bloque de texto claro XJ de longitud N=64 bits. La operación de agrupación que se realiza en la unidad de agrupación 704 es la OR-exclusiva o XOR bit a bit de tal modo que $SJ \oplus WTJv \rightarrow XJ$.

Este bloque de texto claro XJ se suministra por salida 715, formada por 64 líneas paralelas, a la unidad de salida 302.

El bloque de texto claro XJ es convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido a la unidad de destino 105, la cual obtiene el texto claro $\underline{X}$ tras realizarse todo el proceso con la secuencia $\underline{Ys}$.

Al final de la desencriptación con el dispositivo de desencriptación 502v4 del texto aleatorizado-encritpado $\underline{Ys}$ con la clave de desencriptación o bloque seleccionado de control Ksv2, se obtiene el texto claro $\underline{X}$ objeto de la encriptación con el dispositivo de aleatorización-encriptación 501v4 haciendo uso de la clave de aleatorización-encriptación o bloque de control Ksv2.

FIG.7 muestra la segunda realización del dispositivo de aleatorización-encriptación objeto la patente principal nº 9801037 incluyendo la segunda realización de las mejoras. En la FIG.7, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.8 de la patente principal, y FIG.3 y FIG.5 de la presente memoria son designadas por mismas referencias alfanuméricas con objeto de facilitar las referencias.

En esta variante de la unidad de aleatorización-encriptación 501v5, las mejoras adicionales se concretan con respecto a la FIG.3 de la presente memoria por la substitución adicional de la unidad generadora de bloque transformador 1002v y bloque transformador WTI por unidad generadora de bloque transformador 5002v y bloque transformador WTIv respectivamente, así como la eliminación adicional de la entrada/salida 614.

Se describe a continuación las mejoras que son incorporadas.

La unidad generadora de bloque transformador 5002v presenta salida 613, formada por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 5002v suministrar el bloque transformador WTIv de longitud N=64 bits que se suministra como entrada de la unidad de agrupación 603 por entrada 613. La unidad generadora de bloque transformador 5002v genera el bloque transformador WTIv a partir de bloque inicial de control R. El bloque inicial de control R de longitud preferentemente L3=G bits en esta realización está prefijado para la aleatorización-encriptación de una secuencia de texto claro X, no depende del bloque de control Kpv que se suministra por el canal 107 al dispositivo de aleatorización-encriptación 501v5.

La unidad generadora de bloque transformador 5002v implementa función F', tal que genera el bloque transformador WTIv a partir del bloque inicial de control R al igual que la unidad generadora de bloque transformador 5002 de la FIG.5. Así mismo, la función F' que implementa la unidad generadora de bloque transformador 5002v puede ser igual a la función F' que implementa la unidad generadora de bloque transformador 5002 de la FIG.5, pudiendo implementar la misma cualquiera de las opciones que se han descrito previamente de la propia función F'. La diferencia estriba en que el bloque inicial de control R está prefijado en el dispositivo de la FIG.7, mientras que en el dispositivo de la FIG.5 es suministrado por la unidad divisora de bloque de control 1001, unidad no presente en esta realización.

En esta realización, al igual que en las realizaciones previas, se consigue la ventaja referente al desconocimiento por parte de enemigos del bloque transformador a ser agrupado en la unidad de agrupación 603 con el bloque de datos XI, pero no en cambio la ventaja de usar una mayor longitud de bloque de control, pues, respecto a la realización de la patente principal, ésta no sufre cambios.

No se realiza la descripción del dispositivo al considerarse que la similitud con

la descripción ofrecida en el modo de realización de la FIG.5 y la propia FIG.7 permiten comprender cual es el modo de funcionamiento del mismo.

Al igual que los dispositivos de aleatorización-encriptación de las FIG.6 y FIG.8 de la patente principal y FIG.1, FIG.3 y FIG.5 de la presente memoria, el dispositivo de aleatorización-encriptación de la FIG.7 puede ser también utilizado como generador de secuencias de números aleatorios; suministrando diferentes datos de entrada como texto claro X una secuencia de números aleatoria es suministrada como salida Yp.

FIG.8 muestra el dispositivo de desencriptación correspondiente al dispositivo de aleatorización-encriptación de la FIG.7. En la FIG.8, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.9 de la patente principal, y FIG.4 y FIG.6 de la presente memoria son designadas por mismas referencias alfanuméricas con objeto de facilitar las referencias.

En esta variante de la unidad de desencriptación 502v5, las mejoras adicionales se concretan con respecto a la FIG.3 de la presente memoria por la substitución adicional de la unidad generadora de bloque transformador 2002v y bloque transformador WTJ por la unidad generadora de bloque transformador 6002v y bloque transformador WTJv respectivamente, así como la eliminación adicional de unidad 702 y entradas/salidas 712 y 713.

Se describe a continuación las mejoras que son incorporadas.

La unidad generadora de bloque transformador 6002v presenta salida 714, formada por 64 líneas paralelas, siendo el propósito de la unidad generadora de bloque transformador 6002v suministrar el bloque transformador WTJv de longitud N=64 bits que se da como entrada de la unidad de agrupación 704 por entrada 714. La unidad generadora de bloque transformador 6002v genera el bloque transformador WTJv con bloque inicial de control R. El bloque inicial de control R de longitud preferentemente L3=G bits en esta realización está prefijado para la desencriptación de la secuencia de texto aleatorizado-encriptado Ys, no depende del bloque de control Ksv que se suministra por el canal 108, y debe ser igual al bloque inicial de control R utilizado en el dispositivo de la FIG.7 con que se aleatorizó-encriptó la secuencia de texto aleatorizado-encriptado Ys objeto de la desencriptación.

La unidad generadora de bloque transformador 6002v implementa función F', tal que genera el bloque transformador WTJv a partir del bloque inicial de control R,

al igual que la unidad generadora la de bloque transformador 5002v de la FIG.7. La función F' que implementa la unidad generadora de bloque transformador 6002v es igual a la función F' que se usó en la unidad generadora de bloque transformador 5002v del dispositivo de la FIG.7 con que se aleatorizó-encriptó la secuencia de texto aleatorizado-encriptado Ys objeto de la desencriptación.

El dispositivo de la FIG.8 muestra la necesidad del uso del bloque transformador WTJv para poder realizar la desencriptación de la secuencia de texto aleatorizada-encriptada Ys, bloque transformador WTJv que al no ser accesible ni conocido hace más difíciles los ataques para descubrir la secuencia de texto claro X, o la clave de aleatorización-encriptación o bloque seleccionado de control Ksv usado.

La implementación específica de las mejoras de los dispositivos de aleatorización-encriptación y desencriptación, al igual que los dispositivos de las FIG.6, FIG.7, FIG.8 y FIG.9 de la patente principal pueden ser realizados de diferentes modos y puede depender en varios factores como la aplicación que se hará de los mismos, el entorno, la tecnología usada y accesible, etcétera. Una implementación software que se ejecute en computadores electrónicos puede ser dada. Por otra parte, una implementación hardware puede ser también dada en la que las funciones lógicas elementales están en forma de unidades de circuitos independientes que pueden ser construidos de elementos chip discretos o preferentemente de varios módulos de integracion en gran escala ("very large scale integration o VLSI"); microprocesadores usando Memoria Solo de Lectura ("Read Only Memory" o "ROM"), o Memoria Solo de Lectura Programable ("Programmable Read Only Memory" o "PROM"), o Memoria Solo de Lectura Electrónicamente Borrable ("Electronically Erasable Read Only Memory" o "EEROM"); entre muchas implementaciones posibles. La implementación hardware tiene la ventaja sobre la implementación software que puede trabajar substancialmente mas rápido.

Todo cuanto no afecte, altere, cambie o modifique la esencia de las mejoras descritas será variable a los efectos de esta solicitud de adición.

REIVINDICACIONES

1. Mejoras en la patente principal nº 9801037 por "Dispositivo de aleatorización-encriptación de secuencia de datos", aleatorizador-encriptador concebido para generar con mencionada secuencia de datos, secuencia de salida substancialmente aleatoria haciendo uso de bloque de control libremente seleccionable, del tipo compuesto por:

medios de primera entrada para recibir mencionada secuencia de datos,

medios de segunda entrada para recibir mencionado bloque de control,

medios ensambladores de bloques de datos de longitud N que ensambla bloque de datos de longitud N de mencionada secuencia de datos recibida por mencionados medios de primera entrada,

medios divisores de bloque de control que dividen mencionado bloque de control recibido por mencionados medios de segunda entrada,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con bloque inicial de control de longitud 2N,

medios agrupadores que agrupan mencionado bloque de datos de longitud N con bloque de agrupación de longitud N, generando interbloque de longitud N, donde mencionados medios agrupadores incluyen operación OR-exclusiva,

medios de encriptación que agrupan mencionado interbloque de longitud N con mencionados subbloques de control de longitud M, generando bloque de salida de longitud N, donde mencionados medios de encriptación incluyen dispositivo de encriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios suministradores de bloque de salida de longitud N que suministran mencionado bloque de salida de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos aleatorizados-encriptados de salida correspondiente a mencionada secuencia de datos recibida por mencionados medios de primera entrada,

caracterizadas porque

mencionados medios divisores de bloque de control dividen mencionado

bloque de control recibido por mencionada segunda entrada en mencionado bloque inicial de control de longitud 2N, suministrado a mencionados medios generadores de subbloques de control de longitud M, y en bloque inicial de control de longitud G,

mencionado bloque de agrupación de longitud N es bloque transformador de longitud N generado por medios generadores de bloque transformador de longitud N con mencionado bloque inicial de control de longitud G, suministrado por mencionados medios divisores de bloque de control, y con mencionado bloque de salida de longitud N, suministrado por mencionados medios suministradores de bloque de salida de longitud N.

2. Mejoras de acuerdo con la reivindicación 1 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N).

3. Mejoras de acuerdo con la reivindicación 2 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N) para el enésimo mencionado bloque transformador de longitud N es igual a enésimo bloque funcional de longitud N generado por función E_n (mencionado bloque inicial de control de longitud G) XOR enésimo menos uno mencionado bloque de salida de longitud N.

4. Mejoras de acuerdo con la reivindicación 3 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) definible por E_n (Ri) = (E_{n-1} (Ri) oper B) mod 2^{Qi} donde Qi menor o igual que 64, Ri subbloque de longitud Qi de mencionado bloque inicial de control de longitud G, oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, B valor, mod operación módulo.

5. Mejoras de acuerdo con la reivindicación 4 caracterizadas porque mencionado bloque de control formado preferentemente por 192 bits, mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

6. Mejoras de acuerdo con la reivindicación 3 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) para

generar mencionado bloque funcional de longitud N incluye generador de números aleatorios.

7. Mejoras de acuerdo con la reivindicación 6 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de bloque iniciador de mencionado generador de números aleatorios.

8. Mejoras de acuerdo con la reivindicación 3 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) para generar mencionado bloque funcional de longitud N incluye función de hash.

9. Mejoras de acuerdo con la reivindicación 8 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque de control inicial de longitud G formado preferentemente por cero o más bits.

10. Mejoras de acuerdo con la reivindicación 2 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N)

para enésimo mencionado bloque transformador de longitud N es igual a enésimo menos uno mencionado bloque de salida de longitud N XOR enésimo menos uno mencionado bloque transformador de longitud N generado por función H (mencionado bloque inicial de control de longitud G, enésimo menos dos mencionado bloque de salida de longitud N),

y para primer bloque transformador de longitud N incluye mencionado bloque inicial de control de longitud G.

11. Mejoras de acuerdo con la reivindicación 10 caracterizadas porque mencionado bloque de control formado preferentemente por 192 bits, mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

12. Mejoras de acuerdo con la reivindicación 1 caracterizadas porque

se prevee la posibilidad de prescindir de mencionados medios suministradores de bloque de salida de longitud N que suministran mencionado bloque de salida de longitud N,

mencionados medios generadores de bloque transformador de longitud N

generan mencionado bloque transformador de longitud N con mencionado bloque inicial de control de longitud G suministrado por mencionados medios divisores de bloque de control.

13. Mejoras de acuerdo con la reivindicación 12 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G).

14. Mejoras de acuerdo con la reivindicación 13 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G) para enésimo mencionado bloque transformador de longitud N definible por H_n (Ri) = (H_{n-1} (Ri) oper B) mod 2^{Qi}, donde Qi menor o igual que 64, Ri subbloque de longitud Qi de mencionado bloque inicial de control de longitud G, oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, B valor, mod operación módulo.

15. Mejoras de acuerdo con la reivindicación 14 caracterizadas porque mencionado bloque de control formado preferentemente por 192 bits, mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

16. Mejoras de acuerdo con la reivindicación 13 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G) para generar mencionado bloque transformador de longitud N incluye generador de números aleatorios.

17. Mejoras de acuerdo con la reivindicación 16 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de bloque iniciador de mencionado generador de números aleatorios.

18. Mejoras de acuerdo con la reivindicación 13 caracterizado por mencionada función H (mencionado bloque inicial de control de longitud G) para generar mencionado bloque transformador de longitud N incluye función de hash.

19. Mejoras de acuerdo con la reivindicación 18 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por

128 bits y mencionado bloque inicial de longitud G formado por cero o más bits.

20. Mejoras en la patente principal nº 9801037 por "Dispositivo de aleatorización-encriptación de secuencia de datos" , recuperador de secuencia de datos concebido para recuperar mencionada secuencia de datos de secuencia de datos aleatorizados-encriptados haciendo uso de bloque de control libremente seleccionable, del tipo compuesto por:

medios de primera entrada para recibir mencionada secuencia de datos aleatorizados-encriptados,

medios de segunda entrada para recibir mencionado bloque de control,

medios ensambladores de bloques de datos aleatorizados-encriptados de longitud N que ensamblan bloque de datos aleatorizados-encriptados de longitud N de mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con bloque inicial de control de longitud 2N,

medios contenedores de bloque de datos aleatorizados-encriptados de longitud N para contener mencionado bloque de datos aleatorizados-encriptados de longitud N,

medios de desencriptación que agrupan mencionado bloque de datos aleatorizados-encriptados de longitud N con mencionados subbloques de control de longitud M, generando interbloque de longitud N, donde mencionados medios de desencriptación incluyen dispositivo de desencriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios agrupadores que agrupan mencionado interbloque de longitud N con bloque de agrupación de longitud N, generando bloque de salida de longitud N, donde mencionados medios agrupadores incluyen operación OR-exclusiva,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos de salida correspondiente a mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

caracterizadas porque

mencionados medios divisores de bloque de control dividen mencionado bloque de control recibido por mencionada segunda entrada en mencionado bloque inicial de control de longitud 2N, suministrado a mencionados medios generadores de subbloques de control de longitud M, y en bloque inicial de control de longitud G,

mencionado bloque de agrupación de longitud N es bloque transformador de longitud N generado por medios generadores de bloque transformador de longitud N con mencionado bloque inicial de control de longitud G, suministrado por mencionados medios divisores de bloque de control, y con mencionado bloque de datos aleatorizados-encriptados de longitud N, suministrado por mencionados medios contenedores de bloque de datos aleatorizados-encriptados de longitud N.

21. Mejoras de acuerdo con la reivindicación 20 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G, mencionado bloque de datos aleatorizados-encriptados de longitud N) igual a función H usada por medios generadores de bloque transformador de longitud N que incluye el dispositivo de aleatorización-encriptación con que se ha generado mencionada secuencia de datos aleatorizados-encriptados.

22. Mejoras de acuerdo con la reivindicación 20 caracterizadas porque

se prevee la posibilidad de prescindir de mencionados medios contenedores de bloque de datos aleatorizados-encriptados de longitud N que suministran mencionado bloque de datos aleatorizados-encriptados de longitud N,

mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N con mencionado bloque inicial de control de longitud G suministrado por mencionados medios divisores de bloque de control.

23. Mejoras de acuerdo con la reivindicación 22 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G) igual a función H usada por medios generadores de bloque transformador de longitud N que incluye el dispositivo de aleatorización-encriptación con que se ha generado mencionada secuencia de datos aleatorizados-

encriptados.

24. Mejoras en la patente principal nº 9801037 por "Dispositivo de aleatorización-encriptación de secuencia de datos", aleatorizador-encriptador concebido para haciendo uso de bloque de control libremente seleccionable con mencionada secuencia de datos genera secuencia de salida substancialmente aleatoria del tipo compuesto por:

medios de primera entrada para recibir mencionada secuencia de datos,

medios de segunda entrada para recibir mencionado bloque de control,

medios ensambladores de bloques de datos de longitud N que ensambla bloque de datos de longitud N de mencionada secuencia de datos recibida por mencionados medios de primera entrada,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con mencionado bloque de control recibido por mencionados medios de segunda entrada,

medios agrupadores que agrupan mencionado bloque de datos de longitud N con bloque de agrupación de longitud N, generando interbloque de longitud N, donde mencionados medios agrupadores incluyen operación OR-exclusiva,

medios de encriptación que agrupan mencionado interbloque de longitud N con mencionados subbloques de control de longitud M, generando bloque de salida de longitud N, donde mencionados medios de encriptación incluyen dispositivo de encriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios suministradores de bloque de salida de longitud N que suministran mencionado bloque de salida de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos aleatorizados-encriptados de salida correspondiente a mencionada secuencia de datos recibida por mencionados medios de primera entrada,

caracterizadas porque

mencionado bloque de agrupación de longitud N es bloque transformador de longitud N generado por medios generadores de bloque transformador de longitud N

con bloque inicial de control de longitud G y con mencionado bloque de salida de longitud N suministrado por mencionados medios suministradores de bloque de salida de longitud N.

25. Mejoras de acuerdo con la reivindicación 24 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N).

26. Mejoras de acuerdo con la reivindicación 25 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N) para el enésimo mencionado bloque transformador de longitud N es igual a enésimo bloque funcional de longitud N generado por función E_n (mencionado bloque inicial de control de longitud G) XOR enésimo menos uno mencionado bloque de salida de longitud N.

27. Mejoras de acuerdo con la reivindicación 26 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) definible por $E_n (Ri) = (E_{n-1} (Ri)$ oper B) mod 2^{Qi} donde Qi menor o igual que 64, Ri subbloque de longitud Qi de mencionado bloque inicial de control de longitud G, oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, B valor, mod operación módulo.

28. Mejoras de acuerdo con la reivindicación 27 caracterizadas porque mencionado bloque de control formado preferentemente por 192 bits, mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

29. Mejoras de acuerdo con la reivindicación 26 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) para generar mencionado bloque funcional de longitud N incluye generador de números aleatorios.

30. Mejoras de acuerdo con la reivindicación 29 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de bloque iniciador de mencionado generador de números aleatorios.

31. Mejoras de acuerdo con la reivindicación 26 caracterizadas porque mencionada función E_n (mencionado bloque inicial de control de longitud G) para generar mencionado bloque funcional de longitud N incluye función de hash.

32. Mejoras de acuerdo con la reivindicación 31 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque de control inicial de longitud G formado preferentemente por cero o más bits.

33. Mejoras de acuerdo con la reivindicación 25 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de salida de longitud N)

para enésimo mencionado bloque transformador de longitud N es igual a enésimo menos uno mencionado bloque de salida de longitud N XOR enésimo menos uno mencionado bloque transformador de longitud N generado por función H (mencionado bloque inicial de control de longitud G, enésimo menos dos mencionado bloque de salida de longitud N),

y para primer bloque transformador de longitud N incluye mencionado bloque inicial de control de longitud G.

34. Mejoras de acuerdo con la reivindicación 33 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

35. Mejoras de acuerdo con la reivindicación 24 caracterizadas porque

se prevee la posibilidad de prescindir de mencionados medios suministradores de bloque de salida de longitud N que suministran mencionado bloque de salida de longitud N,

mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N con bloque inicial de control de longitud G.

36. Mejoras de acuerdo con la reivindicación 35 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G).

37. Mejoras de acuerdo con la reivindicación 36 caracterizadas porque

mencionada función H (mencionado bloque inicial de control de longitud G) para enésimo mencionado bloque transformador de longitud N definible por H_n (Ri) = (H_{n-1} (Ri) oper B) mod 2^{Qi}, donde Qi menor o igual que 64, Ri subbloque de longitud Qi de mencionado bloque inicial de control de longitud G, oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, B valor, mod operación módulo.

38. Mejoras de acuerdo con la reivindicación 37 caracterizadas porque mencionado bloque de control formado preferentemente por 192 bits, mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

39. Mejoras de acuerdo con la reivindicación 36 caracterizadas porque mencionada función H (mencionado bloque inicial de control de longitud G) para generar mencionado bloque transformador de longitud N incluye generador de números aleatorios.

40. Mejoras de acuerdo con la reivindicación 39 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de bloque iniciador de mencionado generador de números aleatorios.

41. Mejoras de acuerdo con la reivindicación 36 caracterizado por mencionada función H (mencionado bloque inicial de control de longitud G) para generar mencionado bloque transformador de longitud N incluye función de hash.

42. Mejoras de acuerdo con la reivindicación 41 caracterizadas porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de longitud G formado por cero o más bits.

43. Mejoras en la patente principal nº 9801037 por "Dispositivo de aleatorización-encriptación de secuencia de datos", recuperador de secuencia de datos concebido para recuperar mencionada secuencia de datos de secuencia de datos aleatorizados-encriptados haciendo uso de bloque de control libremente seleccionable, del tipo compuesto por:

medios de primera entrada para recibir mencionada secuencia de datos

aleatorizados-encriptados,

medios de segunda entrada para recibir mencionado bloque de control,

medios ensambladores de bloques de datos aleatorizados-encriptados de longitud N que ensamblan bloque de datos aleatorizados-encriptados de longitud N de mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con mencionado bloque de control recibido por mencionados medios de segunda entrada,

medios contenedores de bloque de datos aleatorizados-encriptados de longitud N para contener mencionado bloque de datos aleatorizados-encriptados de longitud N,

medios de desencriptación que agrupan mencionado bloque de datos aleatorizados-encriptados de longitud N con mencionados subbloques de control de longitud M, generando interbloque de longitud N, donde mencionados medios de desencriptación incluyen dispositivo de desencriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios agrupadores que agrupan mencionado interbloque de longitud N con bloque de agrupación de longitud N, generando bloque de salida de longitud N, donde mencionados medios agrupadores incluyen operación OR-exclusiva,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos de salida correspondiente a mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

caracterizadas porque

mencionado bloque de agrupación de longitud N es bloque transformador de longitud N generado por medios generadores de bloque transformador de longitud N con bloque inicial de control de longitud G y con mencionado bloque de datos aleatorizados-encriptados de longitud N suministrado por mencionados medios contenedores de bloque de datos aleatorizados-encriptados de longitud N.

44. Mejoras de acuerdo con la reivindicación 43 caracterizadas porque

mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G, mencionado bloque de datos aleatorizados-encriptados de longitud N) y mencionado bloque inicial de control de longitud G iguales a función H y bloque inicial de control de longitud G respectivamente, usados por medios generadores de bloque transformador de longitud N que incluye el dispositivo de aleatorización-encriptación con que se ha generado mencionada secuencia de datos aleatorizados-encriptados.

45. Mejoras de acuerdo con la reivindicación 43 caracterizadas porque

se prevee la posibilidad de prescindir de mencionados medios contenedores de bloque de datos aleatorizados-encriptados de longitud N que suministran mencionado bloque de datos aleatorizados-encriptados de longitud N,

mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N con bloque inicial de control de longitud G.

46. Mejoras de acuerdo con la reivindicación 45 caracterizadas porque mencionados medios generadores de bloque transformador de longitud N generan mencionado bloque transformador de longitud N por función H (mencionado bloque inicial de control de longitud G) y mencionado bloque inicial de control de longitud G iguales a función H y bloque inicial de control de longitud G respectivamente, usados por medios generadores de bloque transformador de longitud N que incluye el dispositivo de aleatorización-encriptación con que se ha generado mencionada secuencia de datos aleatorizados-encriptados.

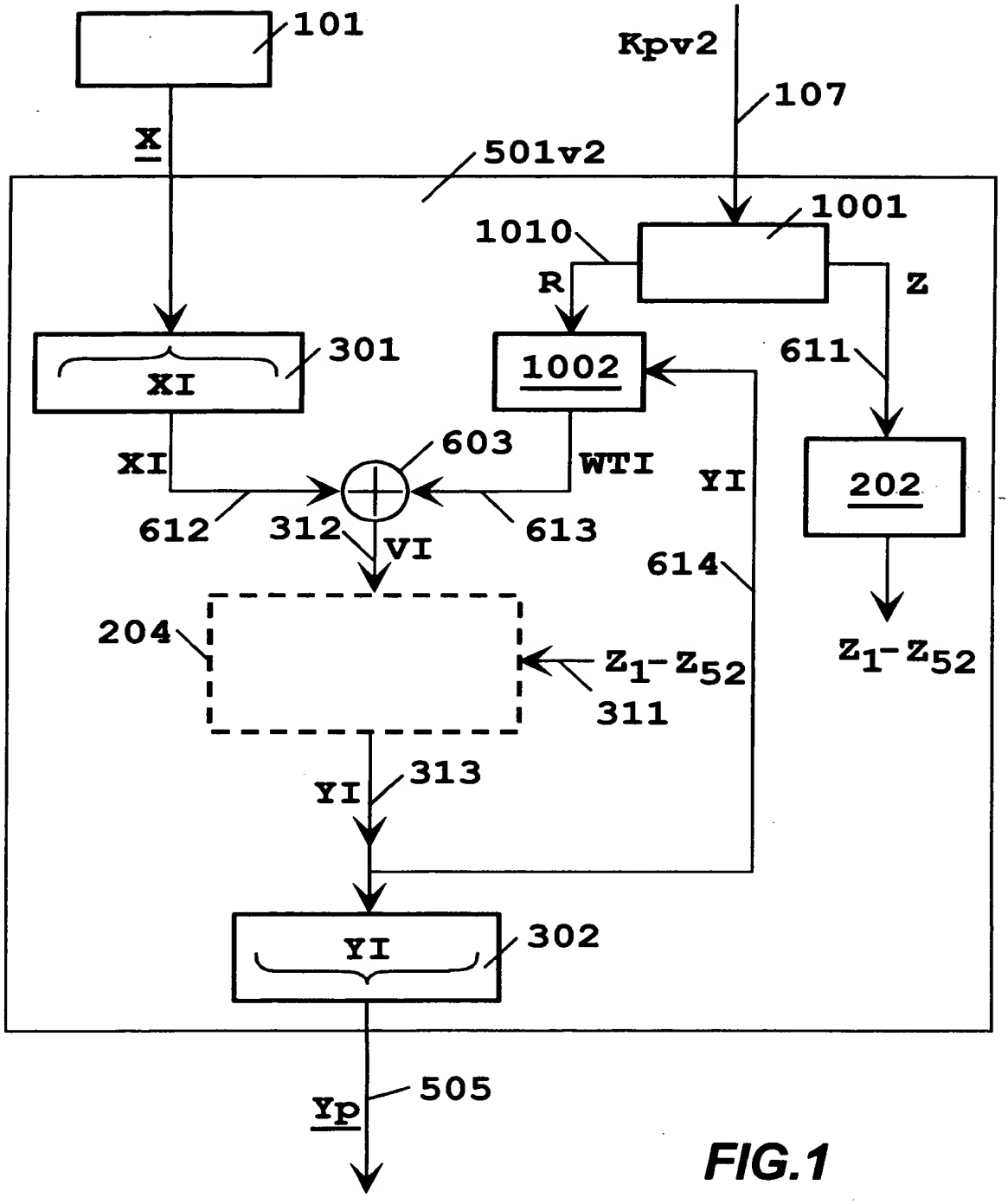
101
Kpv2
107
X
501v2
1001
1010
R
Z
XI
301
1002
611
XI
603
WTI
YI
202
612
312
613
VI
614
204
Z_1-Z_{52}
Z_1-Z_{52}
311
313
YI
YI
302
Yp
505

FIG.1

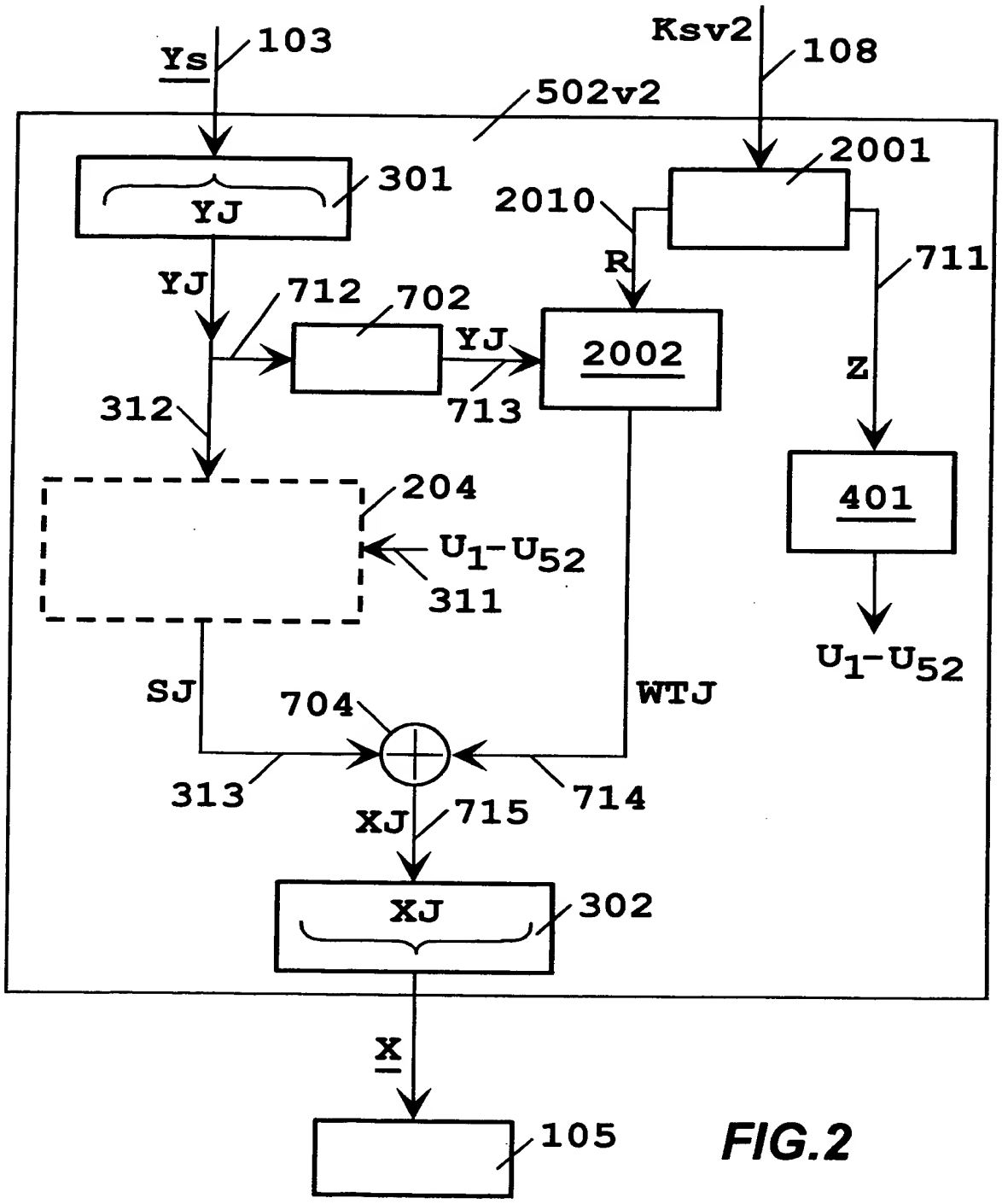
Ksv2
108
Ys
103
502v2
2001
301
YJ
2010
711
R
YJ
712
702
YJ
2002
Z
713
312
204
401
U1-U52
311
U1-U52
SJ
704
WTJ
313
714
XJ
715
XJ
302
X
105

FIG.2

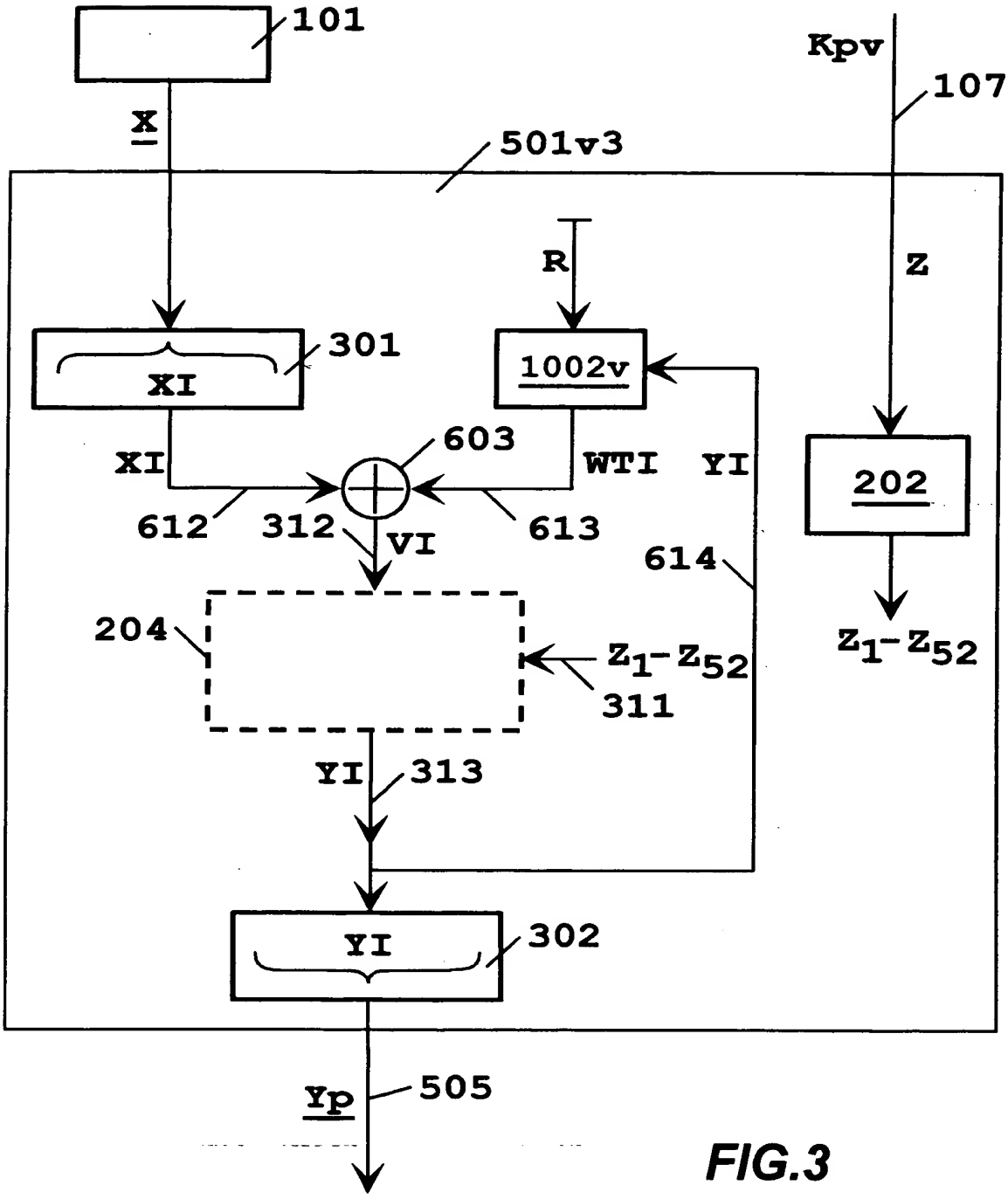
101
X
501v3
Kpv
107
R
Z
301
XI
1002v
603
XI
WTI
YI
202
612
312
VI
613
614
204
Z_1-Z_{52}
311
Z_1-Z_{52}
YI
313
YI
302
Yp
505

FIG.3

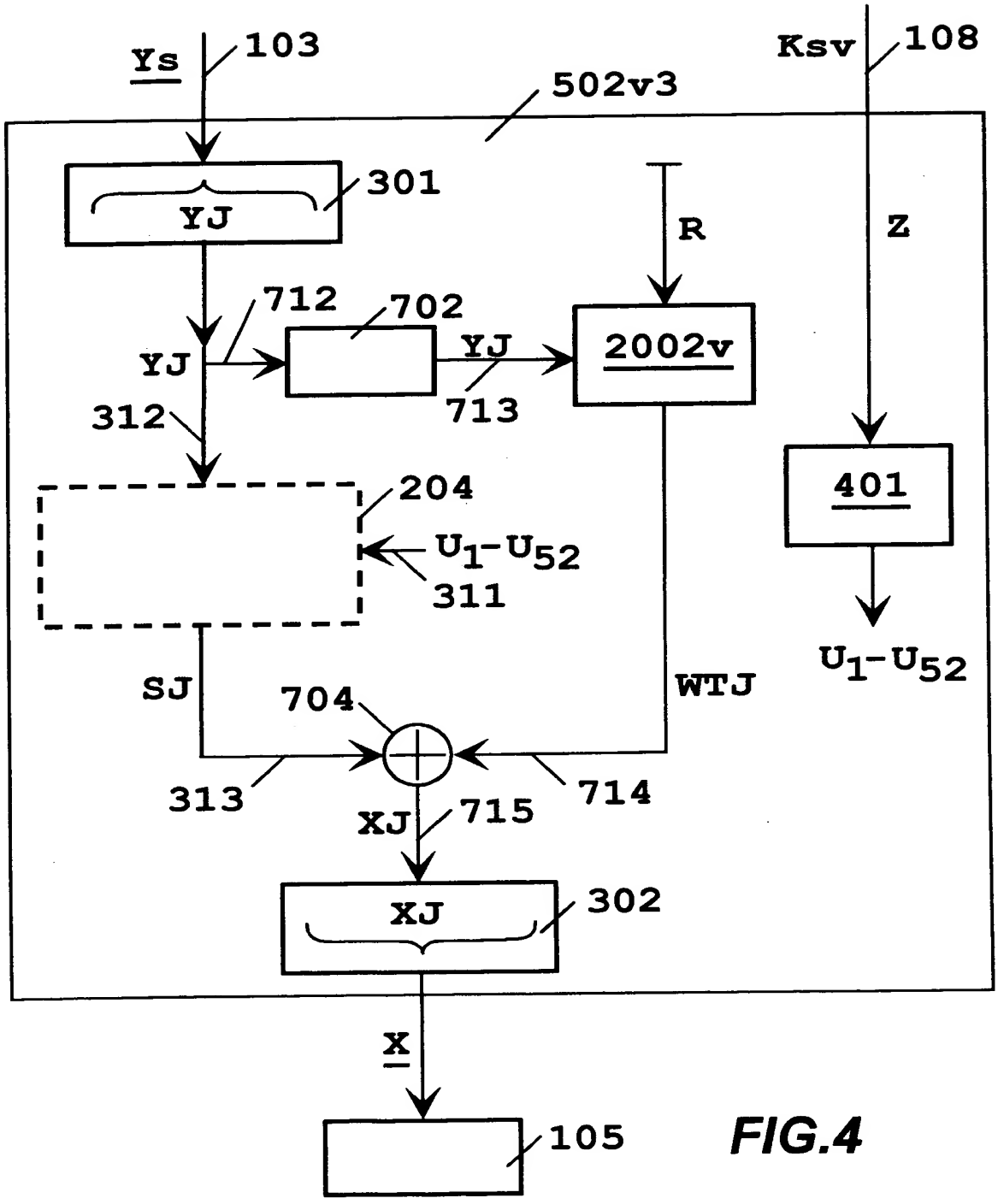
Ys
103
Ksv
108
502v3
301
YJ
R
Z
712
702
YJ
2002v
YJ
713
312
204
U1-U52
311
401
U1-U52
SJ
704
WTJ
313
714
XJ
715
302
XJ
X
105

FIG.4

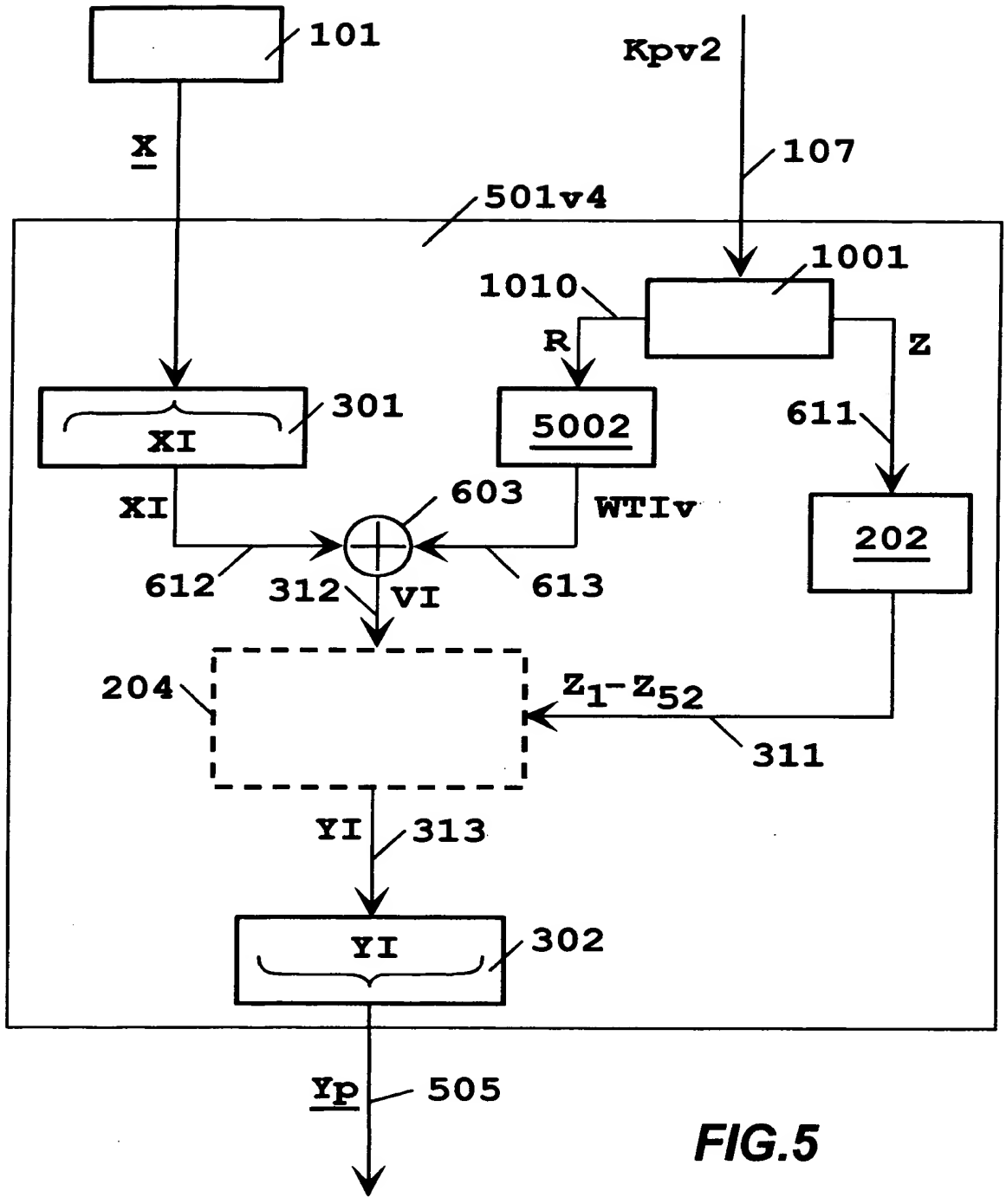
101
Kpv2
X
107
501v4
1001
1010
R
Z
301
XI
5002
611
XI
603
WTIv
202
612
312
VI
613
204
Z_1-Z_{52}
311
YI
313
YI
302
Yp
505

FIG.5

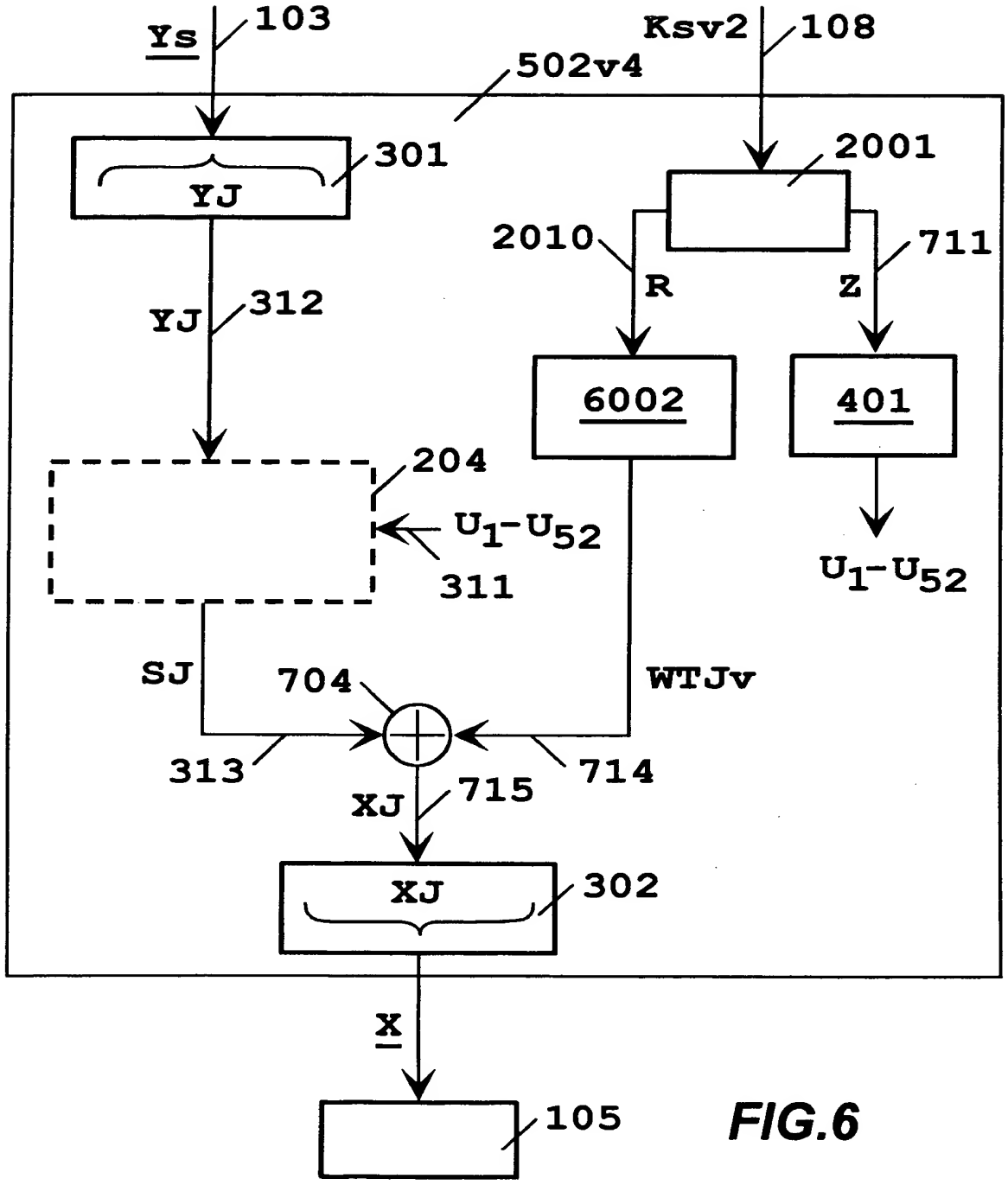
Ys
103
Ksv2
108
502v4
301
YJ
2001
2010
R
Z
711
YJ
312
6002
401
204
U1-U52
311
U1-U52
SJ
704
WTJv
313
714
XJ
715
XJ
302
X
105

FIG.6

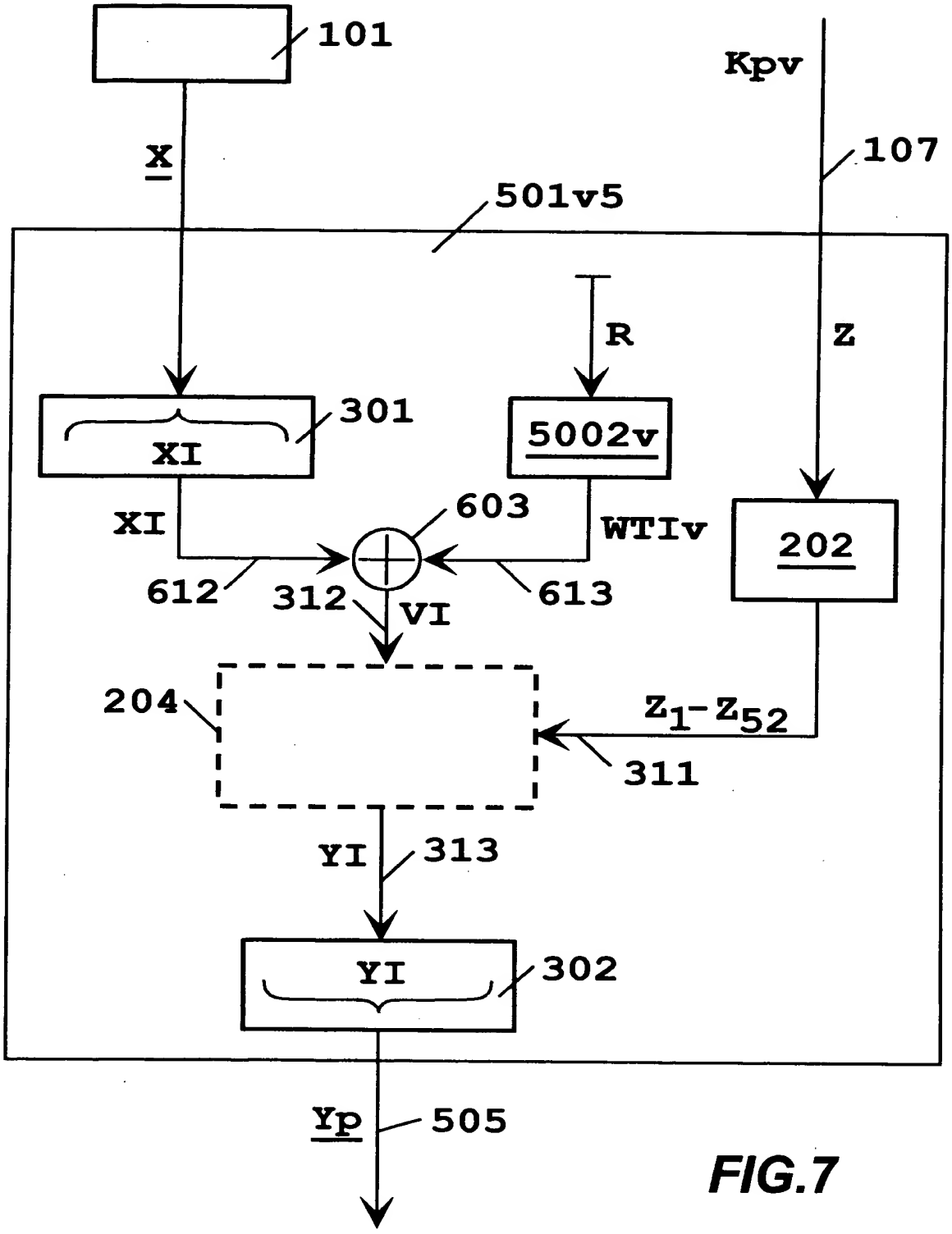
101
Kpv
X
107
501v5
R
Z
301
XI
5002v
XI
603
WTIv
202
612
312
VI
613
204
Z_1-Z_{52}
311
YI
313
YI
302
Yp
505

FIG.7

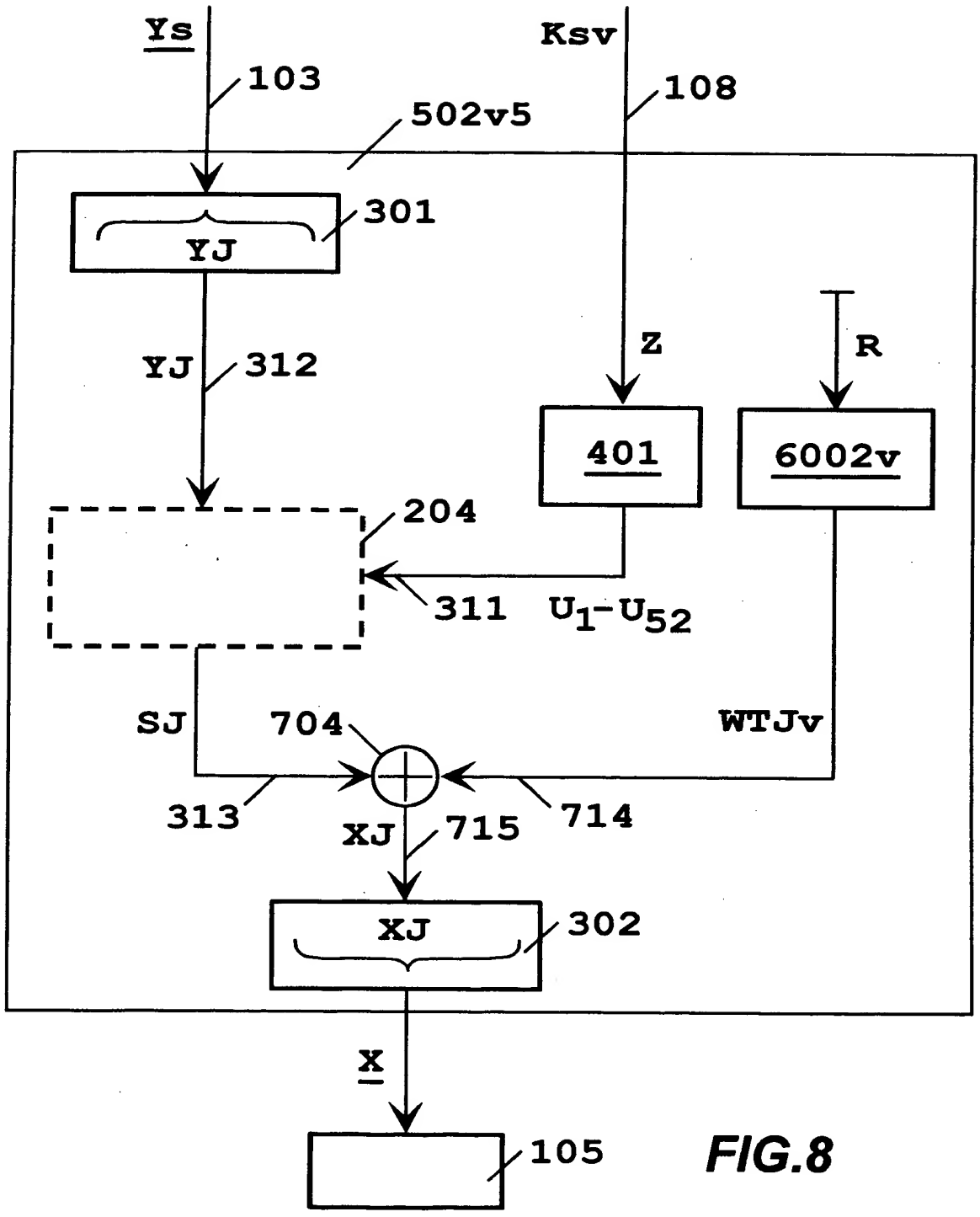
Ys
103
Ksv
108
502v5
301
YJ
YJ
312
Z
R
401
6002v
204
311
U1-U52
SJ
704
WTJv
313
XJ
715
714
XJ
302
X
105

FIG.8